



ENCENTUATE®



# **Encentuate® Identity and Access Management (IAM)**

## ***User Guide***

Product version 3.6

Document version 3.6.3

# Copyright notice

Encentuate<sup>®</sup> IAM User Guide version 3.6.3

Copyright © March 2008 Encentuate<sup>®</sup>. All rights reserved.

The system described in this guide is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Any documentation that is made available by Encentuate is the copyrighted work of Encentuate and is owned by Encentuate.

**NO WARRANTY:** Any documentation made available to you is as is, and Encentuate makes not warranty of its accuracy or use. Any use of the documentation or the information contained herein is at the risk of the user.

Documentation may include technical or other inaccuracies or typographical errors. Encentuate reserves the right to make changes without prior notice.

No part of this document may be copied without the prior written approval of Encentuate.

## Trademarks

Encentuate<sup>®</sup> is a registered trademark in United States of America, Singapore and United Kingdom. Transparent Crypto-Identity, IAM, Encentuate AccessAgent, AccessStudio, Encentuate USB Key and Wallet are trademarks of Encentuate<sup>®</sup>. All other trademarks are the property of their respective owners.

## Contact information

For more information about this product or any support enquiries, contact us:

To log a support incident: <https://customercare.encentuate.com>

To reach us by phone:

■ Americas: +1-800-ENCENTUATE ext 5 (+1-866-362-3688 ext 5)

■ Asia Pacific: +65-6862-7085

Email: [customercare@encentuate.com](mailto:customercare@encentuate.com)

# Table of Contents

---

<b>About This Guide .....</b>	<b>1</b>
Purpose .....	1
Audience .....	1
What's in this guide .....	1
Document conventions .....	2
 <b>IAM Overview .....</b>	 <b>5</b>
About the Encentuate Identity and Access Management Suite .....	5
IAM workflow .....	9
Components of Encentuate IAM .....	9
Encentuate Wallet .....	10
Encentuate AccessAgent .....	10
Encentuate AccessAssistant and Web Workplace .....	10
Encentuate IMS Server .....	11
Encentuate password .....	11
Secret .....	12
USB Key .....	12
Encentuate USB Proximity Key .....	13
Encentuate RFID card .....	13
Encentuate Active Proximity Badge .....	13
Encentuate Fingerprint Identification .....	14
About the Encentuate program icons .....	14
Application icons .....	15
Notification area icons .....	15
 <b>Installing AccessAgent .....</b>	 <b>17</b>
System requirements .....	17
Installing AccessAgent .....	17
Uninstalling AccessAgent .....	19
 <b>Using Encentuate IAM .....</b>	 <b>21</b>
About Single Sign-On (SSO) .....	21
Personal workstation setup .....	22
Signing up to AccessAgent (personal) .....	22
Logging on to AccessAgent (personal) .....	25
Locking and unlocking your computer (personal) .....	25
Shared desktop setup .....	25
Signing up to AccessAgent (shared) .....	25
Logging on to AccessAgent (shared) .....	27
Locking and unlocking your computer (shared) .....	27

Private desktop setup .....	28
Signing up to AccessAgent (private) .....	28
Logging on to AccessAgent (Private) .....	30
Locking and unlocking your computer (private) .....	30
Roaming desktop setup .....	31
Signing up to AccessAgent (roaming) .....	31
Logging on to AccessAgent (roaming) .....	33
Locking and unlocking your computer (roaming) .....	33
Signing up with other enterprise identities .....	34
Using strong authentication .....	34
Passive RFID .....	34
Signing up with your RFID card .....	35
Locking and unlocking your computer (RFID) .....	36
Active RFID .....	36
Signing up with your active RFID card .....	37
Locking and unlocking your computer (active RFID) .....	39
Fingerprint .....	39
Signing up using the fingerprint reader .....	40
Registering more than one finger .....	40
Locking and unlocking your computer (fingerprint) .....	42
USB Key .....	43
Signing up with your USB Key .....	43
Locking and unlocking your computer (USB Key) .....	43
<b>Using Encuentra for Remote Access .....</b>	<b>45</b>
Using Web Workplace .....	45
Signing up (Web Workplace) .....	45
Logging on (Web Workplace) .....	47
Managing applications (Web Workplace) .....	48
Logging on to applications (Web Workplace) .....	48
Capturing user names and passwords (Web Workplace) .....	49
Setting application logon preferences (Web Workplace) .....	50
Setting the default application account (Web Workplace) .....	50
Adding accounts to applications (Web Workplace) .....	50
Editing application passwords (Web Workplace) .....	51
Deleting account from applications (Web Workplace) .....	52
Setting and resetting secrets (Web Workplace) .....	52
Resetting Encuentra passwords (AccessAgent) .....	53
Sending feedback (Web Workplace) .....	57
Getting help (Web Workplace) .....	57
About optional two-factor authentication .....	58
<b>Using Self-Service Features .....</b>	<b>59</b>
Managing Wallets .....	59
Viewing Wallet contents .....	59
About authentication services .....	60
Remembering and storing passwords .....	61
Viewing passwords .....	62
Exporting passwords .....	63
Remembering application passwords .....	63
Adding new users to authentication services .....	64
Searching for credentials within Wallet Manager .....	64

Deleting users from authentication services .....	65
Editing authentication service user names and passwords .....	65
Managing multiple applications for authentication services .....	66
Editing application settings .....	66
Changing Encentuate passwords .....	67
Resetting Encentuate passwords (AccessAgent) .....	68
Resetting self-service secrets (AccessAgent) .....	71
Bypassing strong authentication .....	73
Registering second factor authentication devices after signup .....	73
Using AccessAssistant .....	74
Signing up from AccessAssistant .....	75
Logging on using AccessAssistant .....	76
Logging on to applications from AccessAssistant .....	77
Adding accounts to applications (AccessAssistant) .....	77
Editing application passwords (AccessAssistant) .....	78
Deleting accounts from applications (AccessAssistant) .....	79
Retrieving passwords (AccessAssistant) .....	79
Optional two-factor authentication .....	80
Resetting secrets (AccessAssistant) .....	80
Resetting Encentuate passwords (AccessAssistant) .....	81
Sending feedback .....	85
Getting help .....	85
<b>Troubleshooting .....</b>	<b>87</b>
AccessAgent-related problems .....	87
Unable to install AccessAgent .....	87
Network connection problems .....	88
Installer cannot find IMS Server .....	89
No encryption pack .....	89
The password is not accepted .....	90
The authorization code is not accepted .....	90
Change password problems .....	91
Entries do not match .....	91
Password length .....	91
No network connection .....	91
I cannot remember my Windows user name and password .....	91
Unable to sign up for an Encentuate Wallet .....	92
The temporary Wallet's validity period has expired .....	93
The Encentuate Wallet has been locked .....	93
USB Key-related problems .....	93
Unable to unlock the computer with a USB Key .....	93
Lost Encentuate USB Key .....	93
Unable to remember the password .....	94
Unable to log on to the Wallet .....	94
Unable to register a USB Key .....	94
USB Key is already registered .....	94
The USB Key has been revoked .....	94
RFID card-related problems .....	95
Lost Encentuate RFID card .....	95
Unable to remember the password .....	95
Unable to log on to the Wallet .....	95
Unable to register the RFID card .....	95

RFID card is already registered .....	95
RFID card has been revoked .....	96
Active Proximity Badge-related problems .....	96
Lost Encentuate Active Proximity Badge .....	96
Unable to remember the password .....	96
Unable to log on to the Wallet .....	96
Unable to register Active Proximity Badge .....	97
Active Proximity Badge is already registered .....	97
Active Proximity Card has been revoked .....	97
Active Proximity Badge cannot be detected .....	97
 Glossary and Abbreviations .....	 99

# About This Guide

---

Welcome to the Encentuate Identity and Access Management (IAM) User Guide.

Use this user guide to set up and understand the main functionalities of Encentuate IAM.

## Purpose

This guide provides procedures to setting up Encentuate IAM. It aims to cover the functionality and setup options of the product without focusing on internal implementation details (e.g., describes what the product does and how to set it up).

## Audience

The target users for this user guide are both new and experienced users of Encentuate AccessAgent, Encentuate AccessAssistant, and Encentuate Web Workplace. It is assumed that all users have basic computing knowledge, and are familiar with common computer and Windows-related terms.

## What's in this guide

[IAM Overview](#) provides an overview of Encentuate IAM and its main components.

[Installing AccessAgent](#) contains instructions for successfully installing and configuring AccessAgent.

[Using Encentuate IAM](#) provides step-by-step instructions for signing up with AccessAgent, logging on to AccessAgent, locking your computer, and unlocking your computer. The procedures depend on the type of desktop or workstation setup (e.g., personal, shared, private, or roaming) and additional authentication used (e.g., USB Key, RFID card, fingerprint, etc.).

[Using Encentuate for Remote Access](#) provides step-by-step instructions for using Web Workplace and logging on successfully to web-based applications from another computer.

[Using Self-Service Features](#) details some of the self-service functions in Encentuate IAM, or functions that can be managed by individual users without much assistance from an Administrator or Helpdesk user.

[Troubleshooting](#) provides additional information on resolving commonly encountered Encentuate IAM issues.

[Glossary and Abbreviations](#) defines all the commonly-used terms and abbreviations used throughout the guide.

# Document conventions

Refer to this section to understand the distinctions of formatted content in this guide.

## Main interface elements

The following are highlighted in bold text in the guide: dialog boxes, tabs, panels, fields, check boxes, radio buttons, fields, buttons, folder names, policy IDs/names, and keys. Examples are: **OK**, **Options** tab, and **Account Name** field.

## Navigation

All content that helps users navigate around an interface is italicized (e.g., *Start >> Run >> All Programs*)

## Cross-references

Cross-references refer to other topics in the guide that may provide additional information or reference. Cross-references are highlighted in green and display the referring topic's name (e.g., [Document conventions](#)).

## Hyperlinks

Hyperlinks refer you to external documents or web pages that may provide additional information or reference. Hyperlinks are highlighted in blue and display the actual location of the external document or web page (e.g., <http://www.encentuate.com>).

## Scripts, commands, and code

Scripts, commands, or code are those entered within the system itself for configuration or setup purposes, and are usually formatted in a Courier font.



For example:

```
<script language="JavaScript">

<!--

    ht_basename = "index.php";

    ht_dirbase = "";

    ht_dirpath = "/" + ht_dirbase;

//-->

</script>
```

## Tips or Hints



*Tips or hints help explain useful information that would help perform certain tasks better.*

---

## Warnings



*Warnings highlight critical information that would affect the main functionalities of the system or any data-related issues.*

---



# IAM Overview

---

This chapter covers the following topics:

- [About the Encentuate Identity and Access Management Suite](#)
- [IAM workflow](#)
- [Components of Encentuate IAM](#)
- [About the Encentuate program icons](#)

## About the Encentuate Identity and Access Management Suite

The Encentuate® Identity and Access Management (IAM) Suite empowers enterprises to automate access to corporate information, strengthen security, and enforce compliance at the enterprise end-points.

With Encentuate, enterprises can efficiently manage business risk, achieve regulatory compliance, decrease IT costs, and increase user efficiency. Enterprises do not have to choose between strong security and convenience.

The Encentuate IAM Suite delivers the following capabilities – without requiring changes to the existing IT infrastructure:

- Strong authentication for all user groups
- Enterprise single sign-on with workflow automation
- Comprehensive session management ability
- User-centric access tracking for audit and compliance reporting
- Secure remote access for easy, secure access anywhere, anytime
- Integration with user provisioning technologies
- Building a strong digital identity

## **Strong authentication for all user groups**

Encentuate IAM provides strong authentication for all user groups – inside and outside the corporate perimeter – ensuring authorized access to confidential corporate information and IT networks. The solution leverages multi-factor authentication devices, such as USB smart card tokens, building access badges, proximity cards, mobile devices, photo badges, biometrics, and one-time password (OTP) tokens.

In addition to comprehensive support for authentication devices, Encentuate IAM focuses on leveraging existing identification devices and technologies for authentication. Encentuate IAM also provides iTag, a patent-pending technology that can convert any photo badge or personal object into a proximity device, which can be used for strong authentication.

## **Enterprise single sign-on with workflow automation**

With Encentuate Single Sign-On (ESSO), users can enjoy fast access to all corporate applications (e.g., web, desktop, TTY and legacy) and network resources with the use of a single, strong password on personal and shared workstations.

This feature helps enterprises increase employee productivity, lower IT Helpdesk costs, and improve security levels by eliminating passwords and the effort of managing complex password policies.

Encentuate IAM improves time-to-information by up to 85% via SSO and workflow automation on shared and personal workstations. Users can automate the entire access workflow (e.g., application login, drive mapping, application launch, single sign-on, navigation to preferred screens, multi-step logins, etc.).

Single Sign-Off and configurable desktop protection policies ensure protection of confidential corporate applications from unauthorized access. If a user walks away from a workstation without logging out, Encentuate IAM can be configured to enforce inactivity timeout policies (e.g., configurable screen locks, application logout policies, graceful logoff, etc.).

## **Comprehensive session management capability**

As organizations deploy more shared workstations and kiosks, more users can roam and access information from anywhere without returning to their personal PCs. Shared and roaming scenarios pose severe security threats. When users walk away without logging off from workstations or sharing generic logins, they risk exposing confidential information to unauthorized access. Any attempt to tighten security, enforce unique user logins, and comply with regulations leads to users being locked out of workstations, resulting in efficiency losses.

With Encentuate IAM, organizations can increase user convenience and improve information security through session management or fast user switching capabilities, depending on the access needs user groups. Users can quickly sign-on and sign-off to shared workstations without using the time consuming Windows login process, picking up their work where they left off.

Additionally, fast user switching on private desktops allows users to maintain multiple unique user desktops on the same workstation, preserving each user's applications, documents, and network drive mappings.

If a user walks away from a session without logging off, Encentuate IAM can be configured to enforce inactivity timeout policies. Encentuate IAM also supports hybrid desktops where organizations combine different session management capabilities to best meet the needs of their user community.

## **User-centric access tracking for audit and compliance reporting**

With Encentuate IAM's Audit & Compliance functionality, organizations can consolidate data and manage user-centric, secure, and tamper-evident audit capabilities across all end-points (such as personal or shared workstations, Citrix, Windows Terminal Services, or browsers).

Encentuate's strong authentication capabilities with user-centric audit logs secure access to confidential corporate information and accountability at all times. The logs provide the meta-information that can guide compliance and IT Administrators to a more detailed analysis – by user, by application, or by end-point.

In addition, this information is collated in a central relational database, facilitating real-time monitoring and separate reporting with third party reporting tools.

Organizations can also leverage the end-point automation framework to audit custom access events for any application – without modifying the application or leveraging the native audit functionalities.

## **Secure remote access for easy, secure access anywhere, anytime**

Encentuate Secure Remote Access provides browser-based single sign-on to all applications (e.g., legacy, desktop, and Web) from outside the organization's firewall. Organizations can effectively and quickly enable secure remote access for their mobile workforce without installing any desktop software and modifying application servers.

Remote workers require only one password and an optional second authentication factor to access corporate information from remote offices, home PCs, and PDAs. Once access is granted, users can single sign-on to corporate applications by clicking on the application links available in the Encentuate portal. Access can be further protected through an SSL VPN.

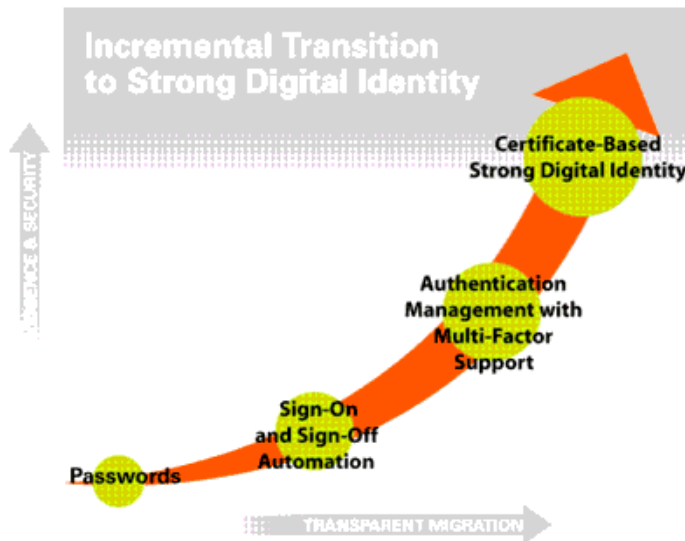
## **Integration with user provisioning technologies**

Encentuate IAM combines with best-of-breed user provisioning technologies to provide end-to-end identity lifecycle management. New employees, partners, or contractors get fast and easy access to corporate information upon being provisioned. Once provisioned, users can leverage single sign-on to access all their applications on shared and personal workstations with one password.

Users are never required to register their user names and passwords individually as their credentials are automatically provisioned.

## Building a strong digital identity

Encentuate IAM combines sign-on and sign-off automation, authentication management and user tracking to provide a seamless path to strong digital identity. Encentuate IAM accelerates the adoption of strong digital identity by transparently increasing security, enhancing user convenience, and providing integrated access across existing information, network and physical systems.



- No change in user behavior
- Incremental, low-risk transition without any user involvement
- Future proof architecture

Encentuate IAM incrementally moves enterprise access from password authentication to strong digital identity-based authentication in the following manner:

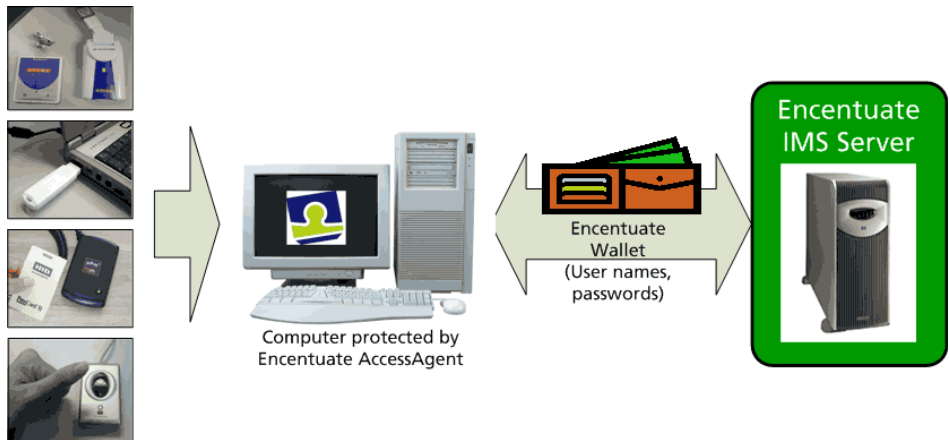
Step 1: Provide sign-on and sign-off automation to enterprise applications

Step 2: Fortify sign-on by using authentication management

Step 3: Provide seamless transition from passwords to certificates

# IAM workflow

The next diagram illustrates a simplified version of the Encentuate IAM workflow.



Encentuate IAM workflow

## Components of Encentuate IAM

The main components of Encentuate IAM are:

- **Encentuate Wallet**
- **Encentuate AccessAgent**
- **Encentuate AccessAssistant and Web Workplace**
- **Encentuate IMS Server**

To use Encentuate AccessAgent, the following must be set:

- **Encentuate password**
- **Secret**

The Encentuate password can be fortified using a second authentication factor. The combination of the password and a USB Key, for example, strengthens the computer's security because both authentication factors must be present to access the computer.

The authentication factors may be used based on an organization's security policy:

- **Encentuate Fingerprint Identification**
- **USB Key**
- **Encentuate USB Proximity Key**
- **Encentuate RFID card**
- **Encentuate Active Proximity Badge**

## Encentuate Wallet

The Encentuate Wallet stores a user's access credentials and related information (including user IDs, passwords, certificates, encryption keys). Each user has a Wallet which is protected by a lock. The lock can be as simple as an Encentuate password, or can be fortified with a second authentication factor.

The Wallet is governed by a set of security policies. The Wallet can be accessed from any end point, either on a workstation where AccessAgent is installed or through a browser.

A "cached" Wallet is an optional copy of the Wallet stored in the hard disk of the computer users sign up with. Users can retrieve the cached Wallet in emergencies, for example, for access without IMS Server connectivity.

In an environment where workstations are regularly shared by several users, one user may have access to several workstations. In that scenario, caching a Wallet saves a lot of time, removing the need to download the Wallet from the IMS Server every time a user accesses another workstation.

## Encentuate AccessAgent

Encentuate AccessAgent is the client software that manages the user's Wallet, enabling automatic sign-on to applications and strong authentication.

## Encentuate AccessAssistant and Web Workplace

Encentuate AccessAssistant is the web-based interface used to provide password self-help. AccessAssistant allows users to obtain the latest credentials to log on to their applications.



Using AccessAssistant, users can access their application passwords from a Web browser without installing AccessAgent on the computer. This feature can be enabled or disabled for the user. Mobile ActiveCode or a Helpdesk-issued authorization code can be used as a second authentication factor for authentication to AccessAssistant.

The Web Workplace is a web-based interface that allows users to log on to enterprise Web applications by clicking on links and not requiring passwords for individual applications. It can be integrated with the customer's existing portal or SSL VPN.

## Encentuate IMS Server

The Encentuate IMS (Integrated Management System) Server is responsible for identity management, certificate management, and audit logs of administrative, user and system actions.

A backup of a user's Wallet contents is stored on the IMS Server, which can be retrieved by connecting to the IMS Server from any computer. The information is encrypted and cannot be read by anyone, including authorized Helpdesk officers and Administrators.

Authorized Administrators are responsible for maintaining the IMS Server.

## Encentuate password

The Encentuate Password is a password six to twenty characters in length, depending on an organization's preference, used to secure access to an Encentuate Wallet. The user specifies a password upon first signup with Encentuate AccessAgent. The enterprise directory password can be used as the Encentuate password.

To sign up with Encentuate AccessAgent means registering with the IMS Server, and creating an Encentuate Wallet. All application credentials are stored in the user's Encentuate Wallet. Signing up ensures the user's credentials are backed up on the server and are retrievable when needed.

The Encentuate Wallet can be associated with a second authentication factor, such as a USB Key, Encentuate Active Proximity Badge, Encentuate RFID card, and others. The second authentication factor reinforces a users' Encentuate Password in protecting the contents of the Wallet.

Follow the following guidelines in choosing a password:

- Choose a lengthy password, not easy to guess, and if possible, a combination of upper and lowercase letters and numbers to avoid having it compromised.
- Do not use dictionary words, a pet's name, the name of a spouse or friend, important dates such as a birth date or an anniversary date as passwords.

- Never tell anyone the password, not even to the Helpdesk officer or Administrator.
- Never write down the password. Change the password as often as possible.

An Encentuate Wallet gets locked after five unsuccessful attempts to log on using an incorrect password. The number of allowed attempts is set by the organization.

## Secret

The user may be asked to enter a secret after signing up for an Encentuate Wallet, depending on the organization's preference. It is similar to the "hint" provided when the user forgets the password for a Web e-mail account. The secret should be something that:

- the user will not forget, even if not used for a long time
- is not likely to change

Upon sign up, the user will also be required to select one or more questions from a list, and then provide the Answer to that question. If the self-service feature is enabled, more than one secret may be required.

In the event of a forgotten Encentuate password, the secret can be used to set a new Encentuate password. The user can also use the secret, along with an authorization code, to gain temporary access to the cached Wallet. The Helpdesk officer will provide the authorization code.

## USB Key

The USB Key is a customized, removable USB drive that combines the utility and storage capacity of Flash RAM, the security of a smart card, and the universal connectivity of Universal Serial Bus (USB) into one package. The USB Key can store user names, passwords, certificates, encryption keys, and other security credentials.



USB Key/USB Proximity Key

# Encentuate USB Proximity Key

The USB Key can be equipped with Radio Frequency Identification (RFID), an electronic device that uses radio frequency signals to read identification information stored within. The USB Key that has RFID integrated within it is called the Encentuate USB Proximity Key.

The USB Proximity Key requires a proximity reader. The proximity reader is installed on the computer for use with Encentuate AccessAgent, or on any other hardware that requires authorization to use. For example, an office front door or elevator can have a proximity reader so that access is restricted to those with an RFID built into their USB Key.

## Encentuate RFID card

An Encentuate RFID card can also be used with the Encentuate password to allow for a more secure, two-factor authentication process.

An Encentuate RFID card also allows for unified access - giving the user access to the computer, as well as for physical security to access doors, elevators, and others.



Encentuate RFID card and reader

## Encentuate Active Proximity Badge

The Encentuate Active Proximity Badge works in almost identical way as the regular RFID card - it has RFID, and works with a proximity reader. However, the Active Proximity Badge differs in the range that it covers.

With the regular Encentuate RFID card, the card needs to be in very close proximity with the reader. With the Active Proximity Badge, the distance can be specified. For example, the Active Proximity Badge can be two meters away from the reader, yet it will be recognized.



Encentuate Active Proximity Badge and reader

## Encentuate Fingerprint Identification

The Encentuate Fingerprint Identification system recognizes the user's fingerprint as an authentication factor. The fingerprint reader translates the fingerprint into encrypted codes, which in turn logs the user on to AccessAgent.





Fingerprint reader

## About the Encentuate program icons




The following icons are used in Encentuate IAM.

# Application icons

Icon	Description
	This icon represents Encentuate AccessAgent application on the desktop.
	This icon represents Encentuate IMS Server on the desktop.

Encentuate IAM application icons

## Notification area icons

Icon	Description
	No user has logged on to AccessAgent.
	AccessAgent is operating normally. When the icon is flashing, AccessAgent is: <ul style="list-style-type: none"><li>■ writing data to the USB Key's smart card</li><li>■ synchronizing a USB Key with the IMS Server</li><li>■ logging the user on</li></ul>
	Single or automatic sign-on is currently disabled.

Encentuate notification area icons



# Installing AccessAgent

---

This chapter covers the following topics:

- [System requirements](#)
- [Installing AccessAgent](#)
- [Uninstalling AccessAgent](#)

## System requirements

Before installing AccessAgent, ensure that the following requirements are met:

- At least an Intel® Pentium® III or equivalent processor
- At least 256MB of RAM
- CD-ROM for installing with an installation CD
- Microsoft Internet Explorer 5 or later

## Installing AccessAgent

There are several ways to install AccessAgent. To know which method to use, contact the Helpdesk officer.



*Retain the default location for the installation files, or click **Browse...** to select a folder in the local drive. Then, click **Next**.*

---

### ■ Using an installation CD

The installation automatically begins once the AccessAgent installation CD is run. If the installation does not begin, access the CD using Windows Explorer and double-click **AccessAgent.msi**.

## ■ Installing with an Encentuate USB Key

The installation files for AccessAgent can be placed in the storage area of the Encentuate USB Key. Insert the USB Key into the port, and access the key using Windows Explorer. Double-click on **AccessAgent.msi** to start the installer.

## ■ Using centralized installation by Administrator

An organization may have a mechanism in place which automatically installs AccessAgent when the user logs on. In this case, no installation screens will be seen except the screen which asks the user to restart the computer.

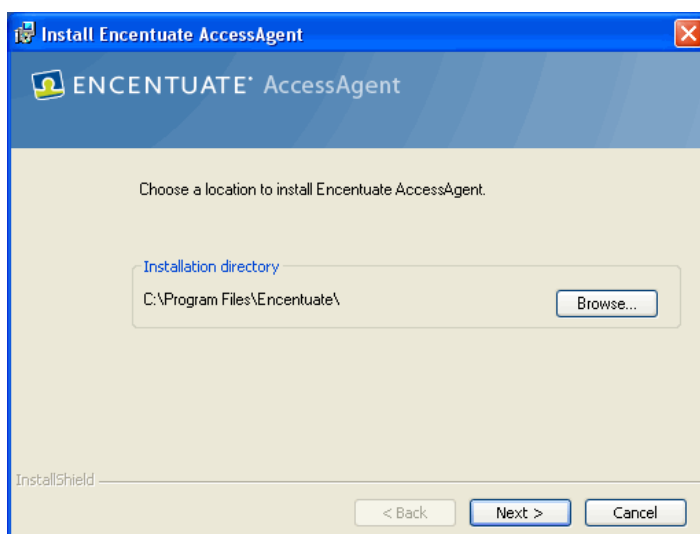


*Ensure that the computer can contact the Encentuate IMS server.*

---

### To install AccessAgent:

- 1 Click on **AccessAgent.msi** to start the installer. The **Install Encentuate AccessAgent** dialog box opens.



InstallShield wizard

- 2 After components have been installed, restart the computer. Click **Yes** to restart immediately, or **No** to restart later.

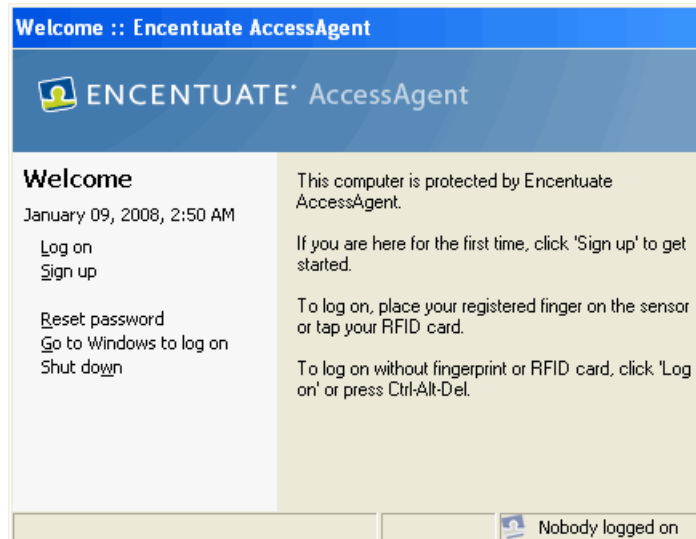


*You cannot sign up or log on to the Wallet during this session, unless the computer restarts.*

---

- 3 After the computer restarts, the AccessAgent welcome window appears. The contents vary according to your organization's preferred settings.





AccessAgent welcome window

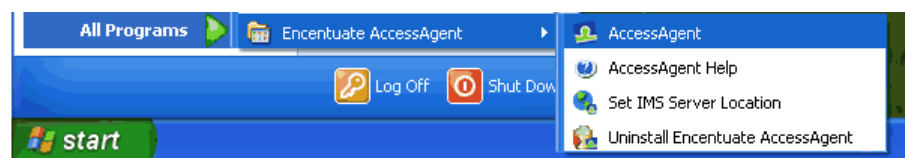
- ④ Choose any of the options listed in the AccessAgent navigation panel on the left side of the window. These options are pre-configured by your Administrator and vary according to user.

If options are not available, contact your Helpdesk officer or Administrator.

# Uninstalling AccessAgent

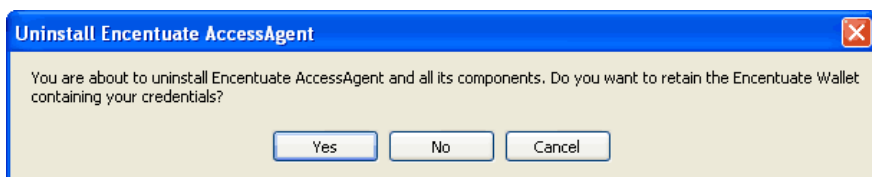
*To uninstall AccessAgent:*

- ① From the Windows **Start** menu, select *All Programs >> Encentuate AccessAgent >> Uninstall Encentuate AccessAgent*. A confirmation window appears.



Windows Start menu - Uninstall Access Agent

- ② Click **Yes** to confirm, or **No** to cancel the uninstallation process.
- ③ If you clicked **Yes**, the Wallet may or may not be cached in the computer. Click **Yes** to keep the Wallet cached, or **No** to remove it. Click **Cancel** to abort the uninstallation process.



Wallet caching confirmation

- 4 Restart the computer.

# Using Encentuate IAM

---

This chapter covers the following topics:

- [About Single Sign-On \(SSO\)](#)
- [Personal workstation setup](#)
- [Shared desktop setup](#)
- [Private desktop setup](#)
- [Roaming desktop setup](#)
- [Signing up with other enterprise identities](#)
- [Using strong authentication](#)

## About Single Sign-On (SSO)

Single sign-on is a capability that allows a user to enter one user ID and password to access multiple applications. Many SSO products are also known as simplified sign-on or reduced sign-on products because they do not support all types of application logons.

Fortified single sign-on (FSSO) is single sign-on with enhanced security capabilities, such as scrambling of passwords (e.g., fortified passwords) and the ability to upgrade the authentication process to use certificates. Encentuate's solution offers fortified SSO via sign-on automation technology that can augment security. Encentuate's single sign-on offering is fortified because:

- Encentuate IAM allows enterprises to choose from several authentication factors (e.g., Encentuate USB Key) to provide two-factor authentication, thus enhancing security.
- Passwords for different applications can be strengthened by automating Encentuate AccessAgent's periodic change of passwords to application-policy aware long randomized strings and storing them in an authentication factor such as the Encentuate USB Key. Users do not have to remember their passwords and they cannot share them to social engineering.

# Personal workstation setup

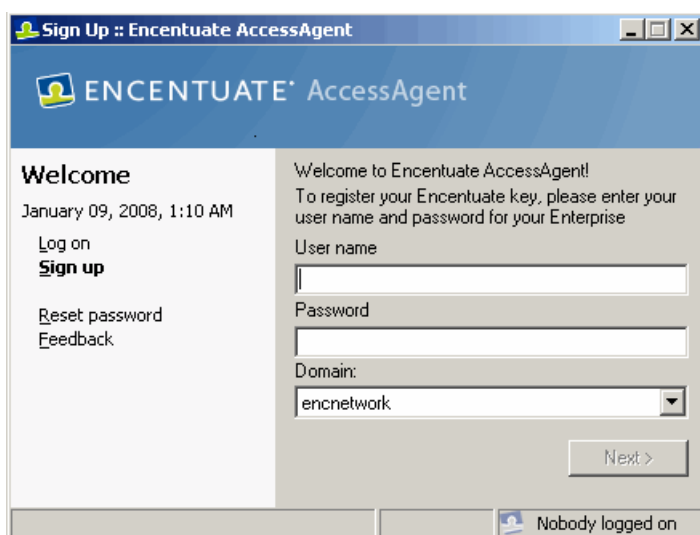
## Signing up to AccessAgent (personal)

Upon signup, be sure to have an enterprise identity or a user name assigned to you by your organization. Your enterprise identity could be your e-mail address, your Active Directory user name, or SAP user name, or any other enterprise directory user name. Encentuate takes your enterprise identity and uses it to label your Encentuate Wallet.

The next steps illustrate the basic sign-up process. The steps may vary, depending on your organization's preferences and the type of workstation configuration to be used.

*To sign up to AccessAgent:*

- ❶ In the AccessAgent navigation panel, click **Sign up**.

The screenshot shows a window titled "Sign Up :: Encentuate AccessAgent". The window has a blue header with the Encentuate logo and the text "ENCENTUATE AccessAgent". On the left side, there is a "Welcome" section with the date and time "January 09, 2008, 1:10 AM" and a list of links: "Log on", "Sign up" (which is highlighted), "Reset password", and "Feedback". On the right side, there is a registration form with the text "Welcome to Encentuate AccessAgent! To register your Encentuate key, please enter your user name and password for your Enterprise". The form includes fields for "User name", "Password", and "Domain" (a dropdown menu currently showing "encnetwork"). A "Next >" button is at the bottom right of the form. At the bottom of the window, there is a status bar that says "Nobody logged on" with a small user icon.

Enter enterprise identity

- ❷ Enter the Windows user name and password. Click **Next**.
- ❸ Enter a password for your Wallet. The new password must match the specified requirements. Confirm your password by entering the new password again in the **Confirm password** field. Click **Next**.

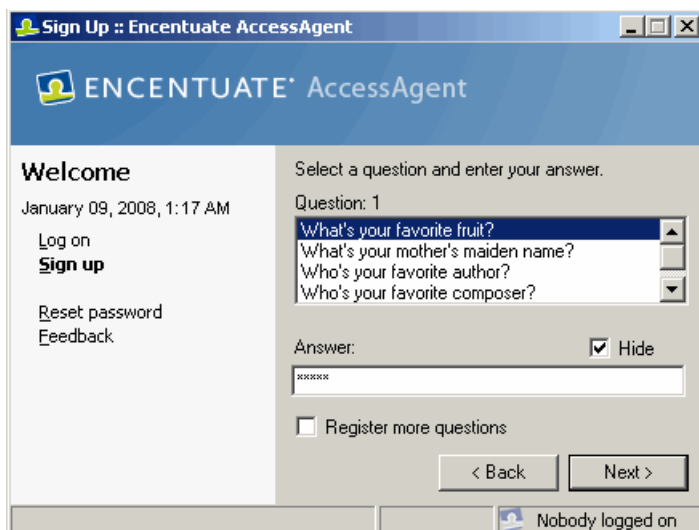
Enter Wallet password

- 4 Select a question and enter the answer. The answer to the secret will be used to retrieve your Wallet contents if you forget your password. Click **Next**.

Select a question and enter the answer

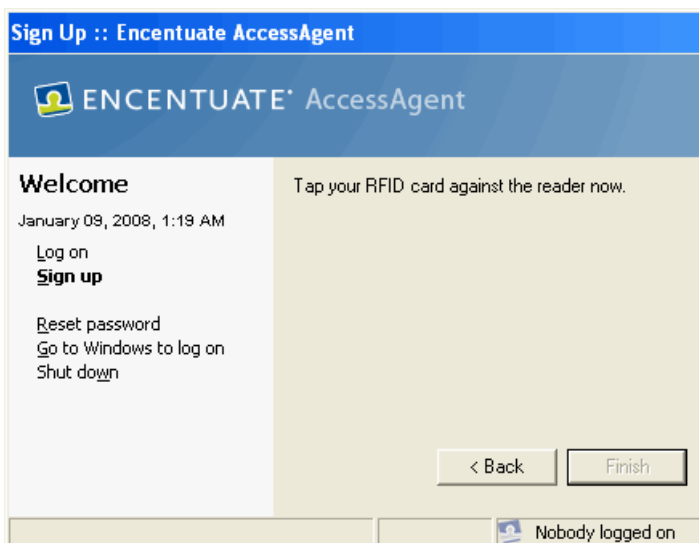
- 5 Select another question and enter the answer. Mark **Hide** if you do not want to display your password. The matching answer to the secret will be used if you forget your password. Click **Next**.

Mark **Register more questions** to add another secret question. Click **Next**.



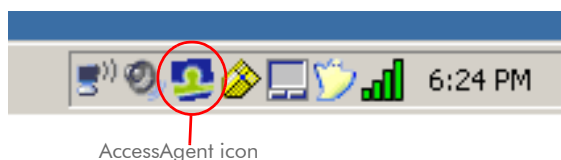
Select another question and enter the corresponding answer

- ⑥ If you are using an authentication device and did not sign-up with it, you will be prompted to use it now. Use your second factor and click **Finish**.



Tap your RFID card

If sign-up is successful, you will see the AccessAgent icon in the notification area of your taskbar.



# Logging on to AccessAgent (personal)

*To log on to AccessAgent:*

- ❶ Turn on the computer.
- ❷ Press **Ctrl+Alt+Del** to log on, or click **Log on** in the AccessAgent navigation panel.
- ❸ Enter your user name and password.
- ❹ Insert or tap your authentication device, if any.

## Locking and unlocking your computer (personal)

If you are going away from your computer, lock your computer using AccessAgent to prevent unauthorized access.

To lock your computer, you can do either of the following:

- Right-click on the AccessAgent icon. From the context menu, select **Lock** this computer.
- Press **Ctrl+Alt+Del** on your keyboard and click **Lock Computer**.
- Double-click on the AccessAgent icon. When the Session information window appears, click **Lock this computer**.

*To unlock your computer:*

- ❶ Click **Unlock this computer** in the navigation panel.
- ❷ Enter your user name and password and click **Next**.

## Shared desktop setup

Shared Desktops allow multiple users to share a generic Windows desktop.

## Signing up to AccessAgent (shared)

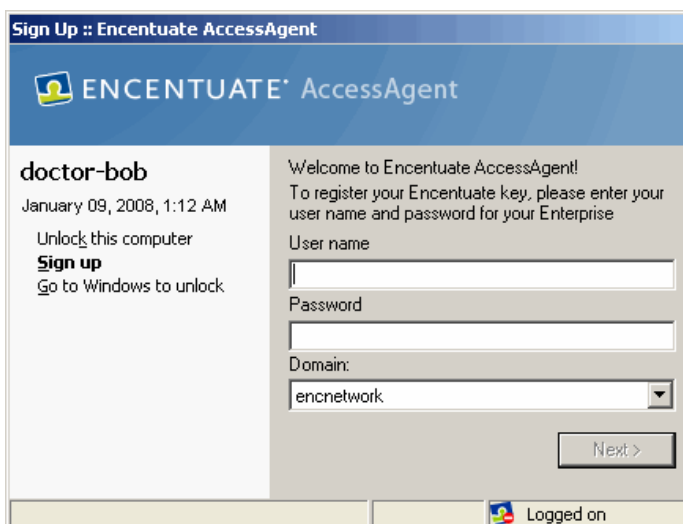
*To sign up to AccessAgent in a Shared Desktop:*

- ❶ In a shared desktop scenario, the previous user, doctor-bob, locks the screen. Click **Sign up** in the AccessAgent navigation panel to use the desktop.



Click Sign-up from the locked screen in a shared desktop scenario

- ② Enter your Windows user name and password. Click **Next**.



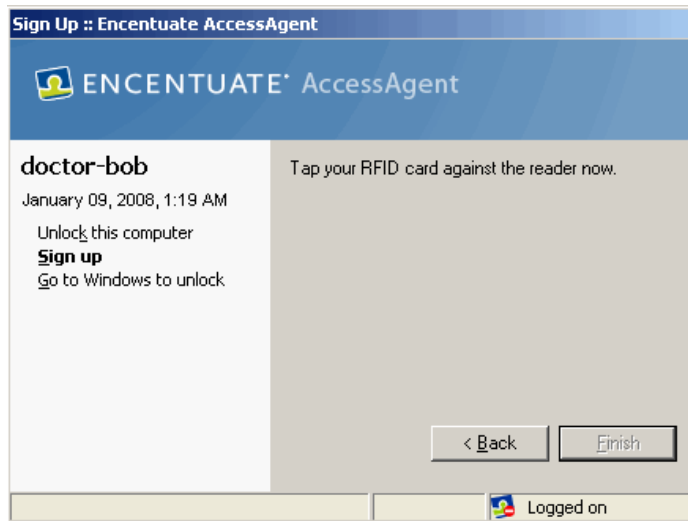
Enter enterprise identity

- ③ Enter a password for your Wallet. The new password must match the specified requirements. Confirm your password by entering the new password again in the **Confirm password** field. Click **Next**.
- ④ Select a question and enter the answer. The answer to the secret will be used to retrieve your Wallet contents if you forget your password. Click **Next**.
- ⑤ Select another question and enter the answer. Mark **Hide** if you do not want to display your password. The matching answer to the secret will be used if you forget your password. Click **Next**.

Mark **Register more questions** to add another secret question. Click **Next**.



- 6 If you are using an authentication device and did not initiate sign-up with it, you will be prompted to use it now. Then, click **Finish**.



Tap RFID card

If sign-up is successful, you will see the AccessAgent icon in the notification area of Windows desktop.



AccessAgent icon

## Logging on to AccessAgent (shared)

*To log on to AccessAgent:*

- 1 From the Computer Locked screen, click **Unlock this computer** in the AccessAgent navigation panel.
- 2 Enter your user name and password.
- 3 Insert or tap your authentication device, if any.

## Locking and unlocking your computer (shared)

If you are going away from your computer, lock your computer using AccessAgent to prevent unauthorized access.

*To lock your computer, you can do either of the following:*

- Right-click on the AccessAgent icon. From the context menu, select **Lock this computer**.
- Press **Ctrl+Alt+Del** on your keyboard and click **Lock this Computer**.
- Double-click on the AccessAgent icon. When the Session information window appears, click **Lock this computer**.

*To unlock your computer:*

- ❶ Click **Unlock this computer** in the navigation panel.
- ❷ Select your user name and enter your password.
- ❸ Click **OK**.

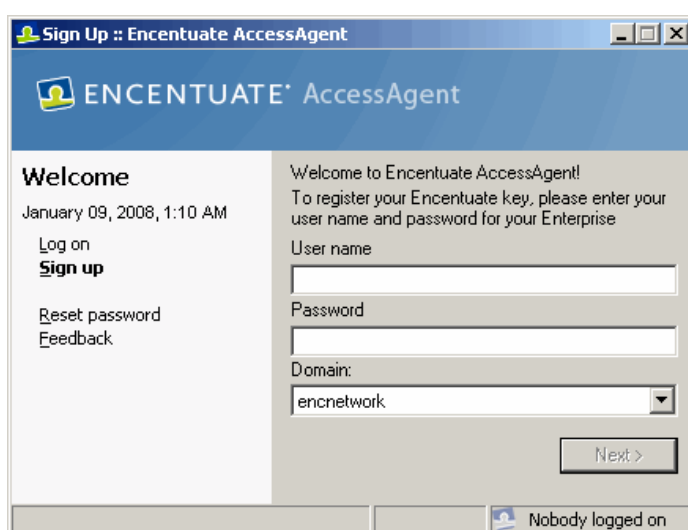
## Private desktop setup

Private Desktops allow multiple users to have their own customized Windows desktops in a workstation.

## Signing up to AccessAgent (private)

*To sign up to AccessAgent in a Private Desktop:*

- ❶ In the AccessAgent navigation panel, click **Sign up**.



The screenshot shows a web browser window titled "Sign Up :: Encentuate AccessAgent". The page has a blue header with the Encentuate logo and "AccessAgent" text. The main content area is divided into two columns. The left column, titled "Welcome", shows the date and time "January 09, 2008, 1:10 AM" and links for "Log on", "Sign up", "Reset password", and "Feedback". The right column, titled "Welcome to Encentuate AccessAgent!", contains a registration instruction: "To register your Encentuate key, please enter your user name and password for your Enterprise". Below this are input fields for "User name", "Password", and "Domain:" (with a dropdown menu showing "encnetwork"). A "Next >" button is at the bottom right. At the very bottom of the window, a status bar shows a user icon and the text "Nobody logged on".

Enter enterprise identity

- ② Enter your Windows user name and password. Click **Next**.
- ③ Enter a password for your Wallet. The new password must match the specified requirements. Confirm your password by entering the new password again in the **Confirm password** field. Click **Next**.
- ④ Select a question and enter the answer. The answer to the secret will be used to retrieve your Wallet contents if you forget your password. Click **Next**.
- ⑤ Select another question and enter the answer. Mark **Hide** if you do not want to display your password. The matching answer to the secret will be used if you forget your password. Click **Next**.

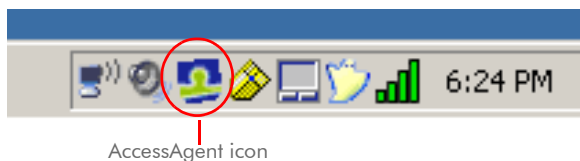
Mark **Register more questions** to add another secret question. Click **Next**.

- ⑥ If you are using an authentication device and **did not** initiate sign-up with it, you will be prompted to use it now. Then, click **Finish**.



Tap RFID card

If sign-up is successful, you will see the AccessAgent icon in the notification area of Windows Desktop.



# Logging on to AccessAgent (Private)

*To log on to AccessAgent:*

- ❶ From the Computer Locked screen, click **Unlock this computer** in the AccessAgent navigation panel.
- ❷ Enter your user name and password.
- ❸ Insert or tap your authentication device, if any.

## Locking and unlocking your computer (private)

If you are going away from your computer, lock your computer using AccessAgent to prevent unauthorized access.

*To lock your computer, you can do either of the following:*

- Right-click on the AccessAgent icon. From the context menu, select **Lock this computer**.
- Press **Ctrl+Alt+Del** on your keyboard and click **Lock this Computer**.
- Double-click on the AccessAgent icon. When the Session information window appears, click **Lock this computer**.

*To unlock your computer:*

- ❶ Click **Unlock this computer** in the navigation panel. Or you can use your second factor to unlock.

Computer Locked :: Encentuate AccessAgent

**ENCENTUATE** AccessAgent

**Computer Locked**  
January 24, 2008, 3:22 AM  
**Unlock this computer**  
[Sign up](#)

Tap your RFID badge, or place your finger on the sensor to unlock.  
User name:  
AAXP1\Administrator  
[...My logon user name is not in the list](#)  
Password:  
OK

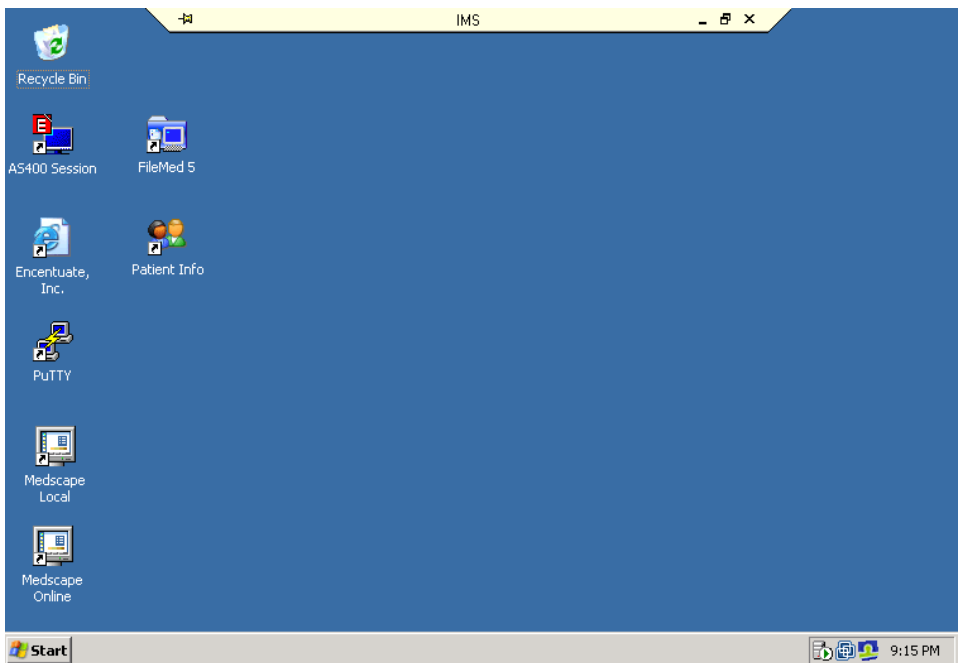
1 user logged on

Tap RFID card

- ② Select your user name and enter your password.
- ③ Click OK.

## Roaming desktop setup

Roaming Desktops allow users' Windows desktops to “roam” to the users' points of access, from workstation to workstation. Roaming Desktops give the user the ability to quickly access and preserve their desktops, regardless of what computer they use.



The remote desktop is distinguished by the terminal session taskbar on the top part of the screen.

## Signing up to AccessAgent (roaming)

*To sign up to AccessAgent on a Roaming Desktop:*

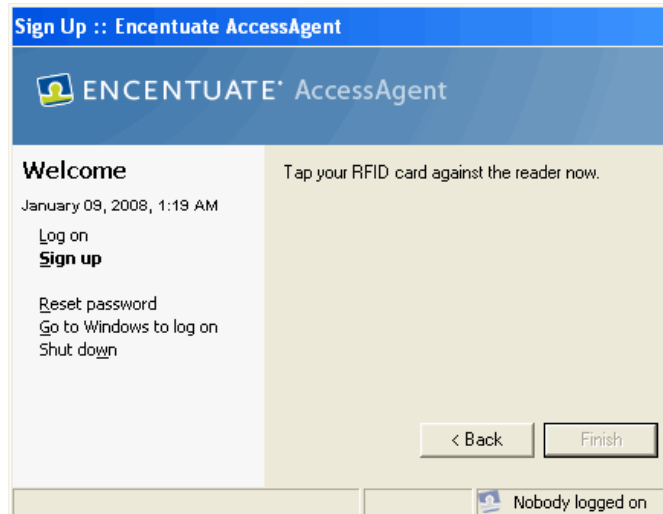
- ① In the AccessAgent navigation panel, click **Sign up**.

Enter enterprise identity

- ② Enter your Windows user name and password. Click **Next**.
- ③ Enter a password for your Wallet. The new password must match the specified requirements. Confirm your password by entering the new password again in the **Confirm password** field. Click **Next**.
- ④ Select a question and enter the answer. The answer to the secret will be used to retrieve your Wallet contents if you forget your password. Click **Next**.
- ⑤ Select another question and enter the answer. Mark **Hide** if you do not want to display your password. The matching answer to the secret will be used if you forget your password. Click **Next**.

Mark **Register more questions** to add another secret question. Click **Next**.

- ⑥ If you are using an authentication device and **did not** initiate sign-up with it, you will be prompted to use it now. Then, click **Finish**.



Tap RFID card

If sign-up is successful, you will see the AccessAgent icon in the notification area of Windows Desktop.



AccessAgent icon

## Logging on to AccessAgent (roaming)

*To log on to AccessAgent:*

- ❶ From the Computer Locked screen, click **Log on** in the AccessAgent navigation panel.
- ❷ Enter your user name and password.
- ❸ Insert or tap your authentication device, if any.

## Locking and unlocking your computer (roaming)

If you are going away from your computer, lock your computer using AccessAgent to prevent unauthorized access.

*To lock your computer, you can do either of the following:*

- Right-click on the AccessAgent icon. From the context menu, select **Lock this computer**.
- Press **Ctrl+Alt+Del** on your keyboard and click **Lock this Computer**.
- Double-click on the AccessAgent icon. When the Session information window appears, click **Lock this computer**.

*To unlock your computer:*

- ❶ Click **Unlock this computer** in the navigation panel.
- ❷ Select your user name and enter your password.
- ❸ Click **OK**.

## Signing up with other enterprise identities

Your organization may opt not to use Active Directory as its enterprise identity. In this case, the Encentuate identity will be bound to an enterprise application directory service (such as Oracle, SAP, PeopleSoft, etc.). Your Encentuate user name and password will be the same as your enterprise application user name and password.

The sign-up sequence for other Enterprise IDs vary according to your organization's deployment preference. Ensure that you follow the onscreen instructions.

## Using strong authentication

### Passive RFID

Passive RFID devices have no internal power source, and only get the power to transmit radio signals from the radio frequency signals they receive. They are only active when a reader is nearby to power them. The lack of an internal power source enables this passive RFID devices to be made very small and are usually embedded into thin identification cards.

The Encentuate RFID card is an example of a passive RFID device.



An Encentuate RFID card can be used with the Encentuate password. The combination of RFID card and password allows for a more secure, two-factor authentication process.

Encentuate RFID card also allows for unified access so can use it to access your computer, as well as for physical security (to access doors, elevators, and others).



Encentuate RFID card and reader

## Signing up with your RFID card

When you are using an Encentuate RFID card as your second-factor authentication method, you will need to initiate the sign-up process with your RFID card.

### *To sign up with your RFID card:*

- ❶ When you see the AccessAgent welcome screen, tap your RFID card on the reader.
- ❷ Click **No** when AccessAgent asks if you already have an Encentuate user name and password.
- ❸ Enter your Windows user name and password. Click **Next**.
- ❹ Enter your New password. The new password must match the specified requirements. Confirm your password by entering the new password once again in the **Confirm password** field and then click **Next**.
- ❺ Select a Secret question and enter the answer. The answer is your secret, which you will use in case you forget your password. Click **Next**.
- ❻ Click **Finish**.

If sign-up is successful, you will see the AccessAgent icon in the notification area of Windows Desktop.

# Locking and unlocking your computer (RFID)

If you are going away from your computer, lock your computer using AccessAgent. This way, nobody can use your computer without your password and RFID card.

The simplest way to lock or unlock your computer is to tap your RFID card on its reader.

## To unlock your computer using your RFID:

- 1 Tap your RFID card on the reader.



*If you leave your computer locked within a specified period of time, you have the option to unlock it by tapping your RFID card on its reader without entering your password. The time limit is set by your Administrator.*

- 2 Enter your Encentuate password.
- 3 Click OK.

## Active RFID

An active RFID device has an internal power source that powers the integrated circuits and broadcast the radio signal to the reader. Because of the internal power source, the active RFID device transmit at a higher power level than a passive device allowing it to broadcast at longer distances and have more applications. They are generally bigger and more expensive to produce. The Encentuate Active Proximity Badge is an example of an active RFID device.



Press this button for a few seconds to switch the badge ON

Press this button for a few seconds to switch the badge OFF

Encentuate Active Proximity Badge On and Off buttons

The Active Proximity Badge works when the badge is within a certain range from the reader. When you walk away from the reader, the computer locks. When your badge is within the reader's range, the computer unlocks given that no obstacles are blocking the area between your badge and the reader.

Your badge will automatically switch off after nine hours of use. When the badge is switched off, the reader does not detect it. You will need to switch it on.

## Signing up with your active RFID card

When you are using an Encentuate Active Proximity Badge as your second-factor authentication method, use Active Proximity Badge to initiate the sign-up process.

### *To sign up with your active RFID card:*

- 1 Turn on and present your Active Proximity Badge.



Present Active Proximity Badge

- 2 In the AccessAgent window, select the badge ID of the badge you want to sign up with by clicking on its number. Click **Register Badge**.



*There may be several badges within range. Make sure you select the one that you are authorized to register. The badge ID is printed on the back of your Active Proximity Badge.*

Select badge to be registered



- ③ Click **No** when AccessAgent asks if you already have an Encentuate user name and password.
- ④ Enter your Windows user name and password. Click **Next**.
- ⑤ Enter your New password. The new password must match the specified criteria. Your new password will not be accepted if it has not fulfilled all the criteria. Confirm your password by entering the new password once again in the Confirm password field and then click **Next**.

- 6 Select a Secret question and enter the answer. The answer is your secret, which you will use in case you forget your password. Click **Finish**.

If sign-up is successful, you will see the AccessAgent icon in the notification area of Windows Desktop.

## Locking and unlocking your computer (active RFID)

The only way to lock or unlock your computer is to move out of or in to the frequency range of the reader.

If you present your Active Proximity Badge within a specified time (e.g., 15 minutes, 30 minutes, etc.), you do not need to enter your password. To find out the duration, contact your Helpdesk officer.

### *To unlock your computer using your Active Proximity Badge:*

- 1 Move within range of the reader.
- 2 Select your user name from the list of available badges.

Computer Locked :: Encentuate AccessAgent

ENCENTUATE AccessAgent

**Welcome**  
January 28, 2008, 4:31 PM  
[Unlock this computer](#)  
[Go to Windows to unlock](#)

Select your badge and enter Encentuate password to log on. If your badge is not registered, select your badge and click Register Badge.

Badge Id: 42930      User name: qa.encentuate.com\doctor-bob

Password:

Register Badge      OK

1 user logged on

Unlock computer

- 3 Enter your Encentuate password.
- 4 Click **OK**.

## Fingerprint

The Encentuate Fingerprint Identification system recognizes your fingerprint as an authentication factor. The fingerprint reader translates your fingerprint into encrypted codes, which logs you on to AccessAgent.

## Signing up using the fingerprint reader

When you use your fingerprint as your second-factor authentication method, place your finger to initiate the sign-up process.

*To sign up using the fingerprint reader:*

- ❶ When you see the AccessAgent welcome screen, place your finger on the fingerprint reader.
- ❷ Click **No** when AccessAgent asks if you already have an Encentuate user name and password.
- ❸ Enter your Windows user name and password. Click **Next**.
- ❹ Place your finger on the fingerprint reader.
- ❺ Click **Finish**.

If sign-up is successful, you will see the AccessAgent icon in the notification area of Windows Desktop.

## Registering more than one finger

Depending on the deployment options of your organization, you can to register more than one finger.

*To register another finger under the same user:*

- ❶ Lock your computer.
- ❷ Place the finger to register on the fingerprint reader.



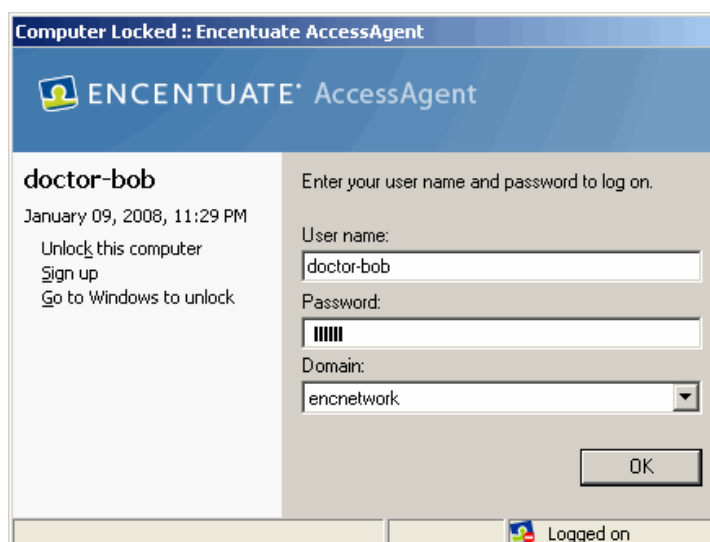
Enter username for fingerprint

- ③ Enter your username when prompted.
- ④ Click **Next**.
- ⑤ Click **Register Fingerprint**.



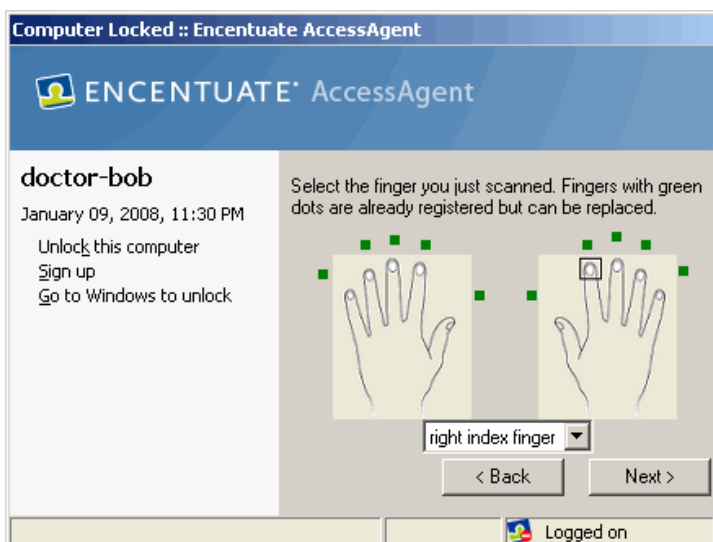
Enter username for fingerprint

- ⑥ Enter your username and password and then click **OK**.



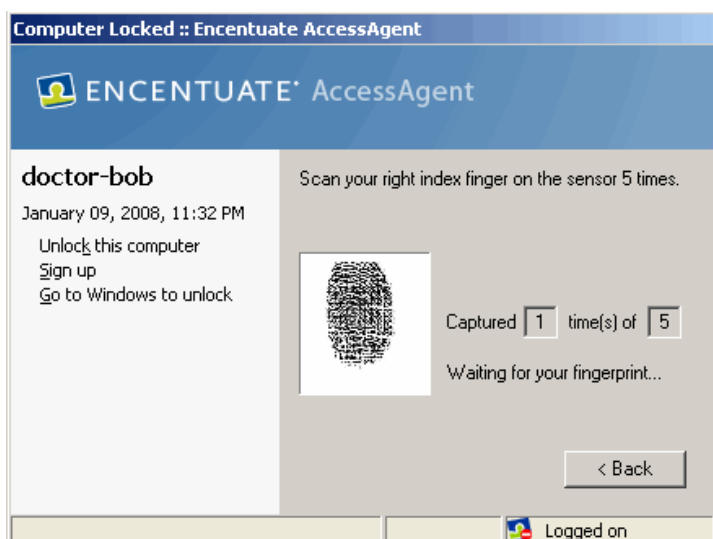
Enter username for fingerprint

- ⑦ Select the finger to register and then click **Next**.



Select finger to register

- 8 AccessAgent require you to scan your finger 5 times to before registering it. Afterwards, you can now use your registered finger for AccessAgent.



Finger to register

## Locking and unlocking your computer (fingerprint)

If you are going away from your computer, lock your computer using AccessAgent. This way, nobody can use your computer without your password and fingerprint.

You can lock your computer by placing your registered finger on the fingerprint reader. To unlock your computer using your fingerprint, place your finger on the fingerprint reader.



# USB Key

The Encentuate USB Key is a customized, removable USB drive that combines the utility and storage capacity of Flash RAM, the security of a smart card, and the universal connectivity of Universal Serial Bus (USB) into one package. Encentuate's USB Key can store user names, passwords, certificates, encryption keys, and other security credentials.

## Signing up with your USB Key

When you use an Encentuate USB Key as your second-factor authentication method, you will need your USB Key to initiate the sign-up process.

*To sign up with your USB Key:*

- ❶ When you see the AccessAgent welcome screen, insert your USB Key in your computer's USB port.
- ❷ Click **No** when AccessAgent asks if you already have an Encentuate user name and password.
- ❸ Enter your Windows user name and password. Click **Next**.
- ❹ Enter your New password. The new password must match the specified requirements. Confirm your password by entering the new password once again in the **Confirm password** field and then click **Next**.
- ❺ Select a Secret question and enter the answer. The answer is your secret, which you will use in case you forget your password. Click **Next**.
- ❻ Click **Finish**.

If sign-up is successful, you will see the AccessAgent icon in the notification area of Windows Desktop.

## Locking and unlocking your computer (USB Key)

If you are going away from your computer, lock your computer using AccessAgent. This way, nobody can use your computer without your password and USB Key. The simplest ways to lock or unlock your computer is to unplug/plug in your USB Key from/into the port.

The following are other ways to lock your computer:

- Right-click on the AccessAgent icon. From the context menu, select **Lock** this computer.
- Press **Ctrl+Alt+Del** on your keyboard and click **Lock Computer**.
- Double-click on the AccessAgent icon. When the Session information window appears, click **Lock this computer**.

*To unlock your computer using your USB Key:*

- ❶ Insert your USB Key into the USB port.
- ❷ Enter your Encentuate password.
- ❸ Click **OK**.

# Using Encentuate for Remote Access

---

This chapter covers the following topics:

- [Using Web Workplace](#)
- [About optional two-factor authentication](#)

## Using Web Workplace

Use Web Workplace to use the automatic sign-on feature without installing AccessAgent on your computer.

Web Workplace is especially useful when you cannot install AccessAgent (e.g., users who need to access enterprise applications through SSL VPN from home computers or cyber cafes). Web Workplace can automatically log the user on to Web-based enterprise applications.

The Web automatic sign-on feature allows users to log on to enterprise Web applications by clicking on links from AccessAssistant, Web Workplace, or enterprise portals, without entering the password of each application.

Users just need to remember one (1) password to log on to all applications. Combined with the reverse proxy feature, Web automatic sign-on can support a large variety of Web applications.

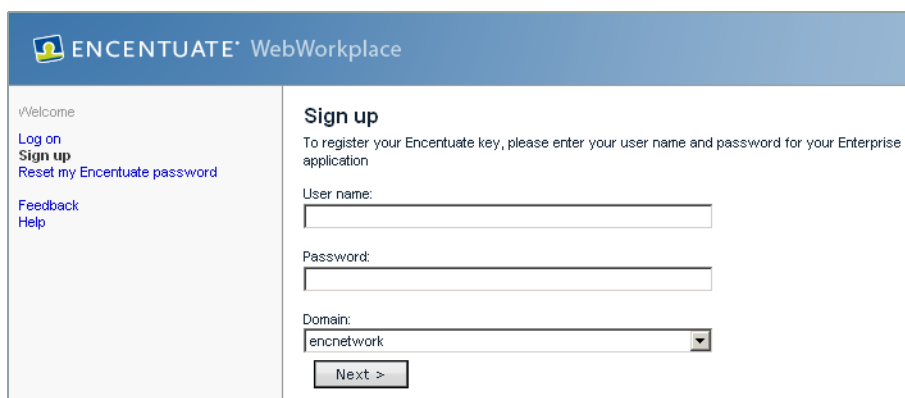
Web Workplace authenticates the Encentuate password. If the Encentuate password is set up to synchronize with the Windows password, users can use their Windows password to log on.

## Signing up (Web Workplace)

When you sign up, you must have an enterprise identity - a user name assigned to you by your organization. Your enterprise identity could be your e-mail address, your Active Directory user name, your SAP user name, etc. Encentuate takes your enterprise identity and uses it to label your Encentuate Wallet.

## To sign up using Web Workplace:

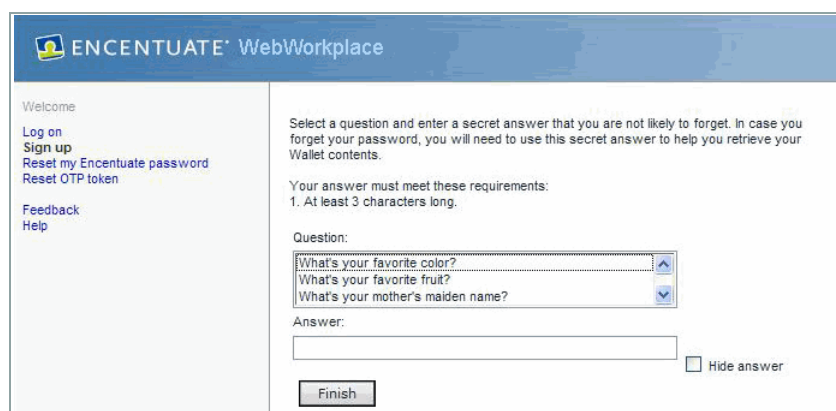
- 1 Go to the URL for Web WorkPlace. Contact Helpdesk if you do not know the URL.
- 2 In the Web Workplace left navigation panel, click **Sign up**.



The screenshot shows the ENCENTUATE WebWorkplace interface. On the left, a navigation panel includes links for Welcome, Log on, Sign up, Reset my Encentuate password, Feedback, and Help. The main area is titled 'Sign up' and contains instructions: 'To register your Encentuate key, please enter your user name and password for your Enterprise application'. It features three input fields: 'User name:', 'Password:', and 'Domain:'. The 'Domain:' field is a dropdown menu currently showing 'encnetwork'. Below these fields is a 'Next >' button.

WebWorkplace Sign up

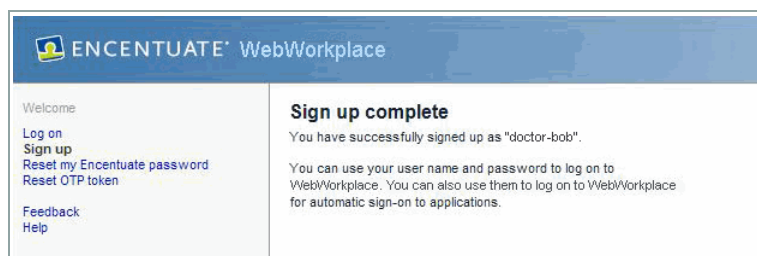
- 3 Enter your Windows user name and password.
- 4 Click **Next**.



The screenshot shows the ENCENTUATE WebWorkplace interface for selecting a secret question. The left navigation panel is the same as in the previous screenshot. The main area is titled 'Select a question and enter a secret answer that you are not likely to forget. In case you forget your password, you will need to use this secret answer to help you retrieve your Wallet contents.' It lists requirements: 'Your answer must meet these requirements: 1. At least 3 characters long.' There is a 'Question:' dropdown menu with three options: 'What's your favorite color?', 'What's your favorite fruit?', and 'What's your mother's maiden name?'. Below this is an 'Answer:' text input field. To the right of the answer field is a checkbox labeled 'Hide answer'. A 'Finish' button is at the bottom.

Selecting a secret question and answer

- 5 Select a question. The answer to this question must be at least three (3) characters long.  
  
If you do not want the answers displayed, mark **Hide answer**.
- 6 Click **Finish**. If signup is successful, you will see a notification on the right panel.



WebWorkplace signup complete

## Logging on (Web Workplace)

By logging on, you have full access to all the application user names and passwords stored in your Wallet. When logged on, you can also use all the features of Web Workplace:

- Web automatic sign-on
- Reverse proxy
- User sign-up
- Manage application credentials (only applications that have AccessProfiles for Web automatic sign-on are listed.)
- Reset secrets
- Reset Encentuate password
- Modify user profile
- Optional two-factor authentication
- Synchronize Wallets, AccessProfiles and policies

*To log on to your Wallet using Web Workplace:*

- ❶ In the Web Workplace left navigation panel, click **Log on**.
- ❷ Enter your Encentuate user name and password. Click **Next >**.

WebWorkplace log on

- ③ Request an authorization code from the Helpdesk and enter the value in the **Authorization code:** field.

Entering an authorization code

- ④ Click **Next**. You can now access Web Workplace features.

## Managing applications (Web Workplace)

### Logging on to applications (Web Workplace)

When you are logged on to Web Workplace, all the enterprise and personal web applications are listed in the right panel of the Web Workplace page. To log on to an application click on the application name. A new browser page opens with the requested application and you are automatically signed on to the application.

encnetwork.local/doctor-bob

[Log off](#)  
**My Web Workplace**  
[Manage AccessProfiles](#)  
[Synchronize system data with IMS Server](#)  
[Reset my secrets](#)

[Feedback](#)  
[Help](#)

### My Web Workplace

Application	User name for automatic logon	
Facebook		<a href="#">Manage &gt;</a>
Google		<a href="#">Manage &gt;</a>
HealthAtoZ	doctorbob	<a href="#">Manage &gt;</a>
Putty	nurse-alice	<a href="#">Manage &gt;</a>
Gmail	javentail	<a href="#">Manage &gt;</a>
Medscape	doctor-bob	<a href="#">Manage &gt;</a>
WebMD	doctor-bob	<a href="#">Manage &gt;</a>
Yahoo web		<a href="#">Manage &gt;</a>

Logging on to applications

## Capturing user names and passwords (Web Workplace)

If the **User name for automatic logon** field is empty, it means that the user name and password for that application have not been captured yet by Web Workplace.

*To capture your user name and password:*

- ❶ Click on the application name.
- ❷ A new window appears, asking you to add your user name and password for that application.

ENCENTUATE WebWorkplace

Please add an account for logging on.

Application:

User name:

Password:


Confirm password:

Capturing application user names and passwords

- ❸ Enter your user name and password.
- ❹ Enter your password again to confirm.
- ❺ Click **Save**.

# Setting application logon preferences (Web Workplace)

Click **Manage** from the **My Web Workplace** screen's right panel to set your application logon preferences. This displays the Manage logon accounts screen.

**ENCENTUATE** WebWorkplace

enclnetwork.localdoctor-bob

[Log off](#)  
[My Web Workplace](#)  
[Manage AccessProfiles](#)  
[Synchronize system data with IMS](#)  
[Server](#)  
[Reset my secrets](#)  
  
[Feedback](#)  
[Help](#)

### Manage logon accounts for "HealthAtoZ"

[< Back to My Web Workplace](#)

User name	Automatic logon		
doctorbob	<input checked="" type="checkbox"/>	<a href="#">Edit password &gt;</a>	<a href="#">Delete</a>

Add user name >


Update

Application logon preferences

If there is only one profile in the application, the **Automatic logon** checkbox is marked by default. If there are two or more applications, you can choose to disable automatic logon to each application.

# Setting the default application account (Web Workplace)

If you have two accounts for the same application, you can set Web Workplace to select the default application account for automatic logon.

**ENCENTUATE** WebWorkplace

enclnetwork.localdoctor-bob

[Log off](#)  
[My Web Workplace](#)  
[Manage AccessProfiles](#)  
[Synchronize system data with IMS](#)  
[Server](#)  
[Reset my secrets](#)  
  
[Feedback](#)  
[Help](#)

### Manage logon accounts for "HealthAtoZ"

[< Back to My Web Workplace](#)

User name	Automatic logon		
doctor-bob2	<input type="checkbox"/>	<a href="#">Edit password &gt;</a>	<a href="#">Delete</a>
doctorbob	<input checked="" type="checkbox"/>	<a href="#">Edit password &gt;</a>	<a href="#">Delete</a>

Add user name >

Update

Setting the default application account

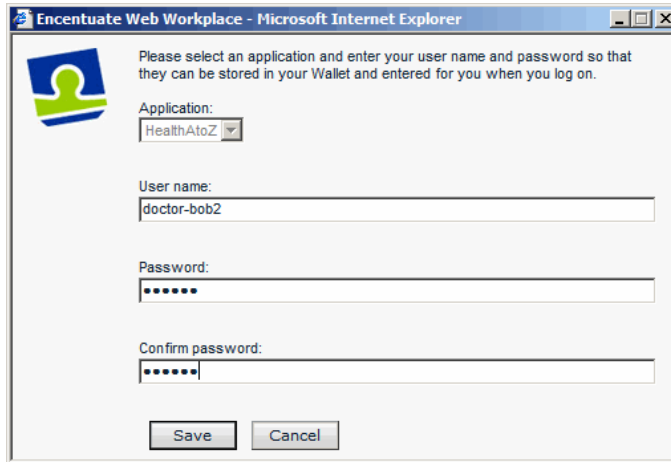
# Adding accounts to applications (Web Workplace)

To add more than one user name for an application, click on the **Add user name** button in the Manage logon accounts page.



*To add another user to an application:*

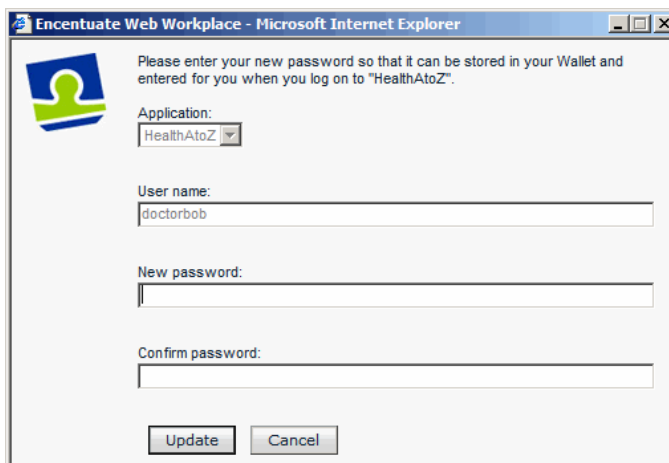
- ❶ In the **Add user account** window, enter the new user name.
- ❷ Enter a password.
- ❸ Enter same password again to confirm.
- ❹ Click **Save**.

The screenshot shows a web browser window titled 'Encentuate Web Workplace - Microsoft Internet Explorer'. The page has a logo on the left and instructional text: 'Please select an application and enter your user name and password so that they can be stored in your Wallet and entered for you when you log on.' Below this, there is a dropdown menu for 'Application:' with 'HealthAtoZ' selected. There are three text input fields: 'User name:' containing 'doctor-bob2', 'Password:' with masked characters, and 'Confirm password:' also with masked characters. At the bottom are 'Save' and 'Cancel' buttons.

Adding another user to an application

## Editing application passwords (Web Workplace)

To change an application's password, click **Edit password** next to the corresponding user name in the Manage logon accounts page.

The screenshot shows a web browser window titled 'Encentuate Web Workplace - Microsoft Internet Explorer'. The page has a logo on the left and instructional text: 'Please enter your new password so that it can be stored in your Wallet and entered for you when you log on to "HealthAtoZ".' Below this, there is a dropdown menu for 'Application:' with 'HealthAtoZ' selected. There are three text input fields: 'User name:' containing 'doctorbob', 'New password:', and 'Confirm password:'. At the bottom are 'Update' and 'Cancel' buttons.

Editing application passwords

*To edit an application's password:*

- ❶ In the Edit password window, enter the new password.
- ❷ Enter the new password again to confirm.
- ❸ Click **Update**.

## Deleting account from applications (Web Workplace)

To delete an application user name and password, click **Delete** next to the corresponding user name in the Manage logon accounts page.

The screenshot shows the ENCENTUATE WebWorkplace interface. On the left is a navigation menu with links: Log off, My Web Workplace, Manage AccessProfiles, Synchronize system data with IMS, Server, Reset my secrets, Feedback, and Help. The main content area is titled 'Manage logon accounts for "HealthAtoZ"' and includes a '< Back to My Web Workplace' link. Below this is a table with columns 'User name' and 'Automatic logon'. The table contains two rows: 'doctor-bob2' with an unchecked checkbox and 'doctorbob' with a checked checkbox. Each row has 'Edit password >' and 'Delete' links. At the bottom are 'Add user name >' and 'Update' buttons.

User name	Automatic logon	
doctor-bob2	<input type="checkbox"/>	<a href="#">Edit password &gt;</a> <a href="#">Delete</a>
doctorbob	<input checked="" type="checkbox"/>	<a href="#">Edit password &gt;</a> <a href="#">Delete</a>

Editing application passwords

## Setting and resetting secrets (Web Workplace)

Web Workplace offers a host of self-service capabilities to the users, such as the ability to reset secret questions and answers. Instead of calling Helpdesk for an authorization code, the self-service feature allows users to reset their Encentuate passwords by specifying answers to secret question(s).

*To reset your secrets:*

- ❶ In the Web Workplace left navigation panel, click **Reset my secrets**.
- ❷ Select a new secret question from the drop-down list.
- ❸ Enter the secret answer. If you do not want the answer to be visible, mark **Hide answer**.

ENCEN TUATE WebWorkplace

encnetwork.local\doctor-bob

[Log off](#)  
[My Web Workplace](#)  
[Manage AccessProfiles](#)  
[Synchronize system data with IMS Server](#)  
**Reset my secrets**  
[Feedback](#)  
[Help](#)

Select 3 different questions and enter your secret answers that you are not likely to forget. In case you forget your password, you will need to use these secret answers to help you retrieve your Wallet contents.

Your answer must meet these requirements:  
1. At least 3 characters long.

Question 1:  
What's your mother's maiden name?  
Answer 1: [Input field with 7 dots] ☒ Hide answer

Question 2:  
What's your favorite fruit?  
Answer 2: [Input field with 4 dots] ☒ Hide answer

Question 3:  
What's your favorite color?  
Answer 3: [Input field with 4 dots] ☒ Hide answer

Resetting secrets

- 4 Specify an optional second secret question and answer.
- 5 Click **Reset** to save the new secret question(s) and answer(s).

If reset is successful, a notification appears in the right panel.

ENCEN TUATE WebWorkplace

encnetwork.local\doctor-bob

[Log off](#)  
[My Web Workplace](#)  
[Manage AccessProfiles](#)  
[Synchronize system data with IMS Server](#)  
**Reset my secrets**  
[Feedback](#)  
[Help](#)

**Reset secret complete**  
You have successfully reset your secrets.

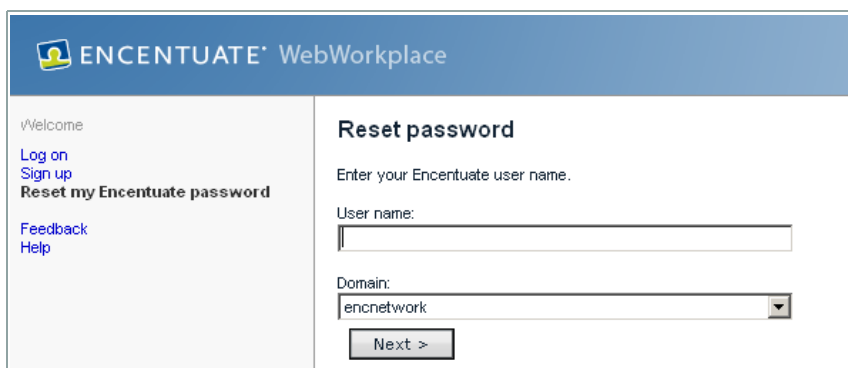
Resetting secret complete

## Resetting Encentuate passwords (AccessAgent)

Use AccessAgent to reset your password when necessary (e.g., when you forget your Encentuate password).

## To reset your Encentuate password (with secret answer):

- 1 In the Web Workplace left navigation panel, click **Reset my Encentuate password**.

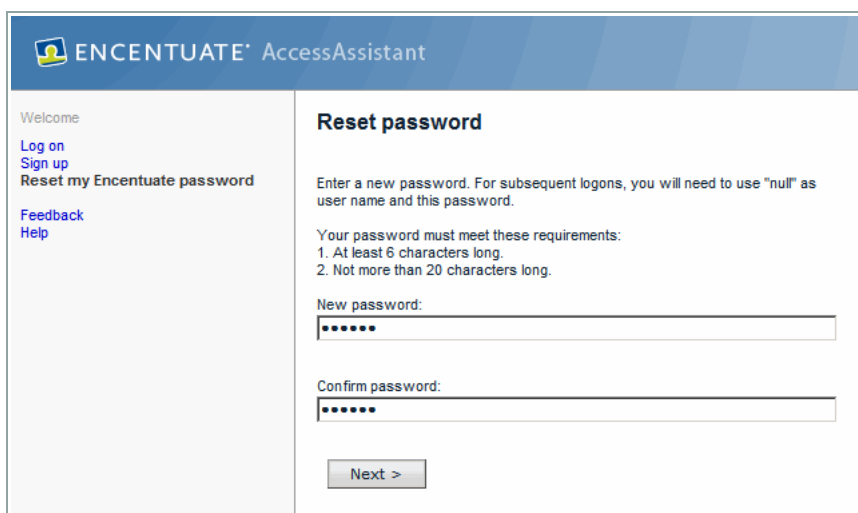


The screenshot shows the 'ENCENTUATE' WebWorkplace interface. On the left, a navigation panel includes links for 'Welcome', 'Log on', 'Sign up', 'Reset my Encentuate password' (highlighted), 'Feedback', and 'Help'. The main content area is titled 'Reset password' and contains the instruction 'Enter your Encentuate user name.' Below this are two input fields: 'User name:' and 'Domain:' (which has 'encnetwork' selected in a dropdown menu). A 'Next >' button is at the bottom.

Resetting the Encentuate password

- 2 Enter your Encentuate user name.
- 3 Click **Next**.
- 4 Enter the secret answers. Provide the correct answers to both secret questions.

If you cannot remember your second or third optional secret answers, refer to the next procedure.



The screenshot shows the 'ENCENTUATE' AccessAssistant interface. The left navigation panel is identical to the previous screen, with 'Reset my Encentuate password' highlighted. The main content area is titled 'Reset password' and contains the instruction 'Enter a new password. For subsequent logons, you will need to use "null" as user name and this password.' It lists requirements: '1. At least 6 characters long.' and '2. Not more than 20 characters long.' Below are two input fields: 'New password:' and 'Confirm password:', both masked with dots. A 'Next >' button is at the bottom.

Resetting the Encentuate password (1/3)

- 5 Click **Next**.

Resetting the Encentuate password (2/3)

- ❶ Enter a new password. The new password must meet the requirements listed on the right panel.
- ❷ Enter the new password again to confirm.
- ❸ Click **Next**. If the password reset is successful, you will see a notification in the right panel.

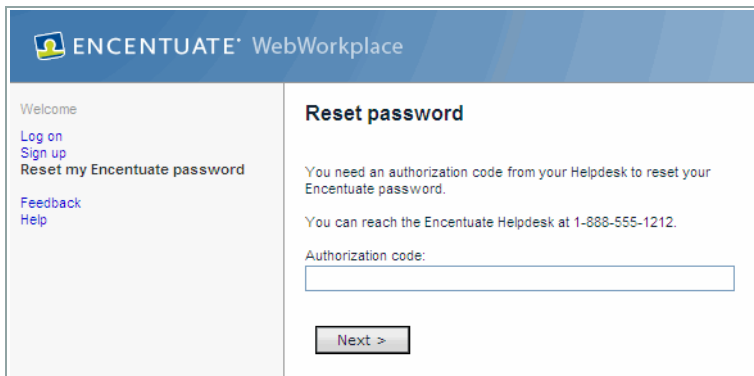
Resetting the Encentuate password (3/3)

If you cannot remember one of your secret answers, you can still reset your Encentuate password with an authorization code issued by Helpdesk.

### *To reset your Encentuate password (with authorization code):*

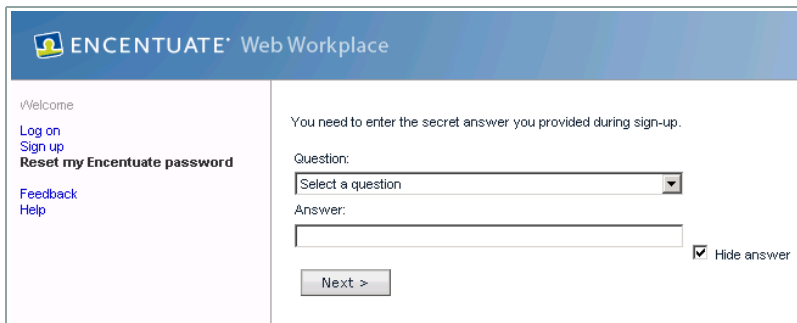
- ❶ In the Web Workplace left navigation panel, click **Reset my Encentuate password**.
- ❷ Enter your Encentuate user name.
- ❸ Click **Next**
- ❹ Enter the secret answer. Provide the secret answers to the other secret questions.
- ❺ Contact Helpdesk to request for an authorization code. The number to contact should be available on your Web Workplace page.

- 6 Enter the authorization code. The authorization code is not case-sensitive.



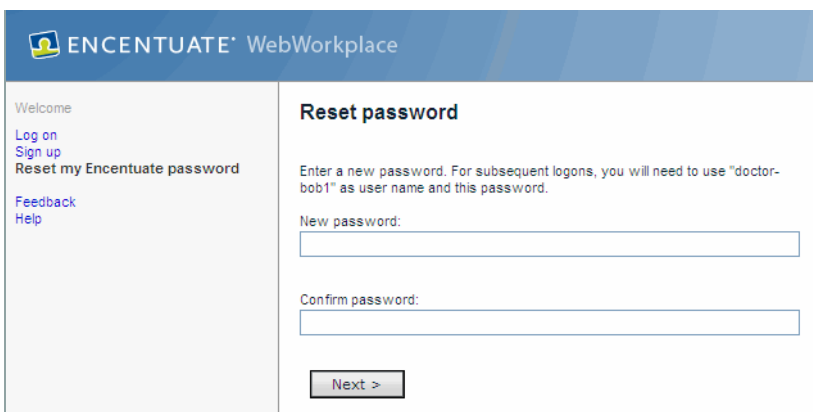
Resetting the Encentuate password (1/3)

- 7 Click **Next**.
- 8 Enter at least one secret answer that you provided during signup.



Resetting the Encentuate password (2/3)

- 9 Click **Next**.
- 10 Enter a new password.
- 11 Confirm the password you have entered.



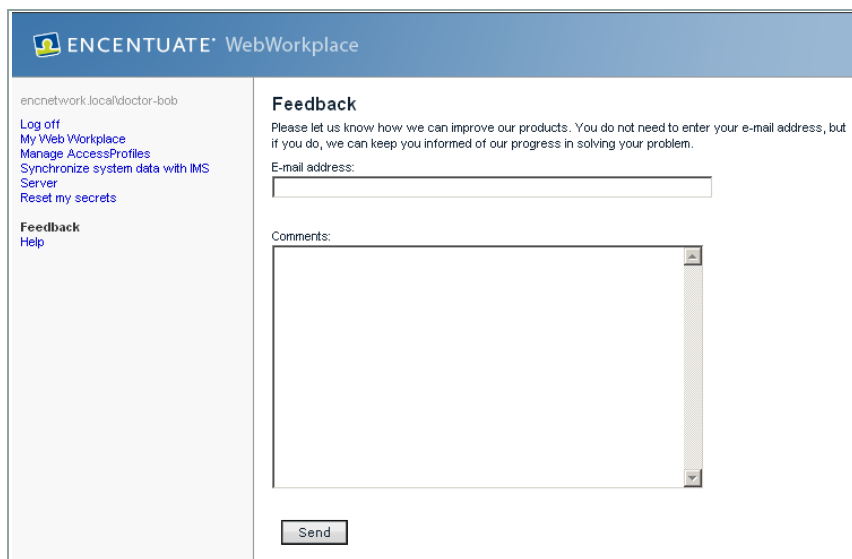
Resetting the Encentuate password (3/3)

- 12 Click **Next**. If password reset is successful, you will see a notification in the right panel.

## Sending feedback (Web Workplace)

*To send feedback about Web Workplace to the Encentuate team:*

- 1 Click **Feedback** in the Web Workplace left navigation panel.
- 2 Enter your e-mail address and comments, then click **Send**.

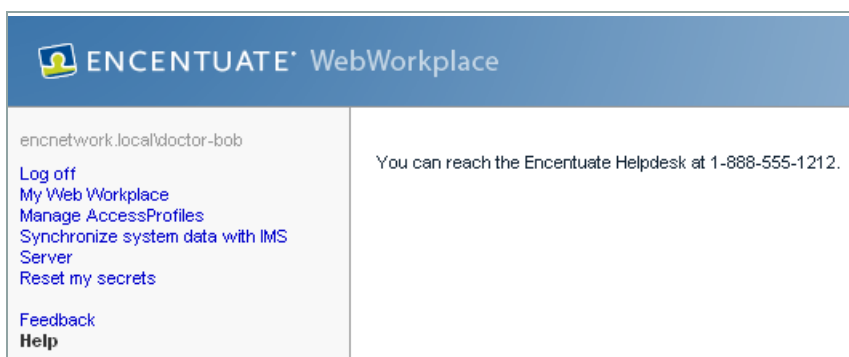


The screenshot shows the 'ENCENTUATE WebWorkplace' interface. On the left is a navigation panel with the user 'encnetwork.local\doctor-bob' and links for 'Log off', 'My Web Workplace', 'Manage AccessProfiles', 'Synchronize system data with IMS', 'Server', 'Reset my secrets', 'Feedback', and 'Help'. The main area is titled 'Feedback' and contains a message: 'Please let us know how we can improve our products. You do not need to enter your e-mail address, but if you do, we can keep you informed of our progress in solving your problem.' Below this is a text input field for 'E-mail address:' and a larger text area for 'Comments:'. A 'Send' button is at the bottom right of the form.

Sending feedback on WebWorkplace

## Getting help (Web Workplace)

If you need help on any of the features of Web Workplace, you can click **Help** in the Web Workplace left navigation panel.



The screenshot shows the 'ENCENTUATE WebWorkplace' interface with the 'Help' option selected in the left navigation panel. The main area displays the text: 'You can reach the Encentuate Helpdesk at 1-888-555-1212.'

WebWorkplace assistance

# About optional two-factor authentication

If two-factor authentication is turned on, you will need to supply one of the following, in addition to your Encentuate password, to log on:

- Authorization code issued by Helpdesk
- Mobile Active Code (MAC), which can be sent to user via mobile phone or email.
- One-time Password (OTP) provided by an OTP token (e.g., VASCO Digipass).



# Using Self-Service Features

---

This chapter covers the following topics:

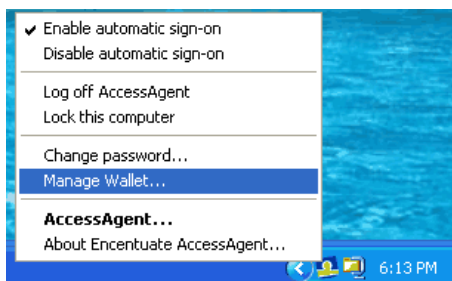
- [Managing Wallets](#)
- [Changing Encentuate passwords](#)
- [Resetting Encentuate passwords \(AccessAgent\)](#)
- [Resetting self-service secrets \(AccessAgent\)](#)
- [Bypassing strong authentication](#)
- [Registering second factor authentication devices after signup](#)
- [Using AccessAssistant](#)

## Managing Wallets

The Wallet Manager manages the passwords stored in your Wallet and allows you to configure the settings for the passwords according to your needs and/or personal preferences.

## Viewing Wallet contents

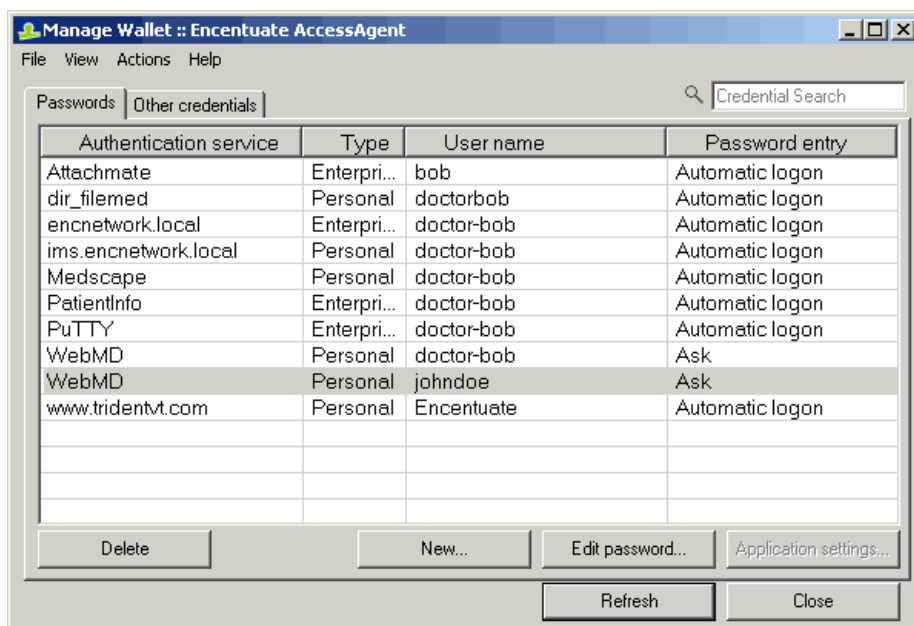
To view your Wallet's contents, right-click on the AccessAgent icon in the notification area, then select **Manage Wallet**.



Manage Wallet option

You can also access your Wallet using the **Manage Wallet** link in the AccessAgent navigation panel.

When you click **Manage Wallet**, the Manage Wallet window is displayed.



Manage Wallet window

## About authentication services

An authentication service verifies the validity of a logon account. It is different from an application, since two applications may authenticate against the same authentication service.

For example, your corporate e-mail can be considered an authentication service, but it can be accessed using many different applications, such as Outlook, Eudora, web mail, and others.

AccessAgent can perform automatic sign-on to all applications you need to access from your computer. With AccessAgent, you only need to remember your Encentuate user name and password.

# Remembering and storing passwords

The **Password Entry** column consists of a drop-down menu with the following options to apply to a password:

Password entry options	Description
Automatic Logon	AccessAgent automatically enters your user name and password. Click <b>OK</b> , then you are logged on to the application(s). You are not required to enter your password as long as password entry is set to automatic logon.
Always	AccessAgent automatically enters your user name and password. To log on to an application, press <b>Enter</b> on your keyboard or click <b>OK</b> .
Ask	AccessAgent prompts the user to use the stored user name and password for the application before logging in.  If the user has more than one account stored, this option can be used to choose the credentials to use for logging on to the application.
Never	Access agent never prompts you to enter your user name and password.
Certificate	Select this option if your application is certificate-enabled. Usually, this option is selected automatically.
Application Settings	You will see this option if you have configured multiple applications for an authentication service.

Password Entry Options

If you have several user names for an authentication service, refer to the table below to learn how you can configure the password entry option.

You Want	Do
To be asked which user name to use	Set password entry to <b>Ask</b> .
To always use one of the user names	Set password entry to <b>Always</b> and the rest to <b>Never</b> .
To never enter any password	Set all user names to <b>Never</b> .
To delete an entry for an application	Select the entry and click <b>Delete</b> .

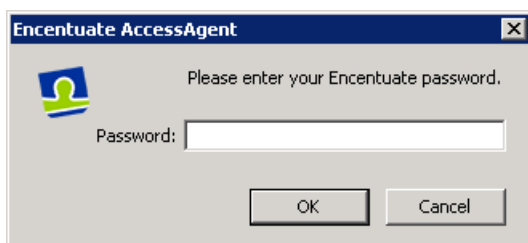
Configuring Password Entry for Multiple User Names

## Viewing passwords

*To view the password for an authentication service:*

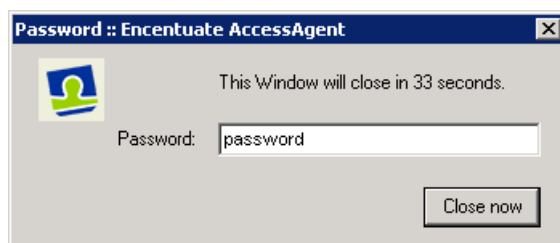
- 1 Click on an entry.
- 2 Go to *Actions >> Show password...*

Alternatively, you can right-click on the entry and select **Show password...**



Entercentuate password dialog box

- 3 Enter your Entercentuate password. The password from the application selected in the Wallet is displayed.

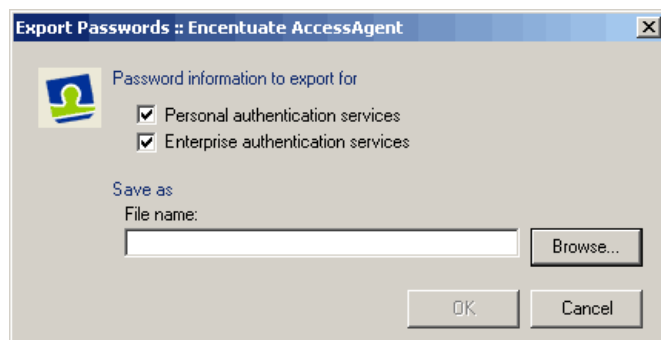


The password is shown only for a few seconds

# Exporting passwords

*To export passwords stored in the Wallet:*

- 1 Go to **File >> Export passwords**. Alternatively, you can click on the **Export passwords** button.

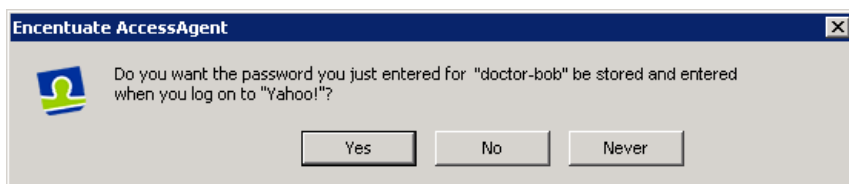


Remember password dialog box

- 2 Mark the appropriate export password options.
- 3 Click **Browse...** to specify the folder that will contain the exported passwords.  
Enter the file name and select the file type of the exported passwords.
- 4 Click **Save**.

## Remembering application passwords

After entering an application user name and password for an application, AccessAgent displays a dialog box and asks whether to store the user name and password for that application.



Remember password dialog box

Click **Yes** to store the user name and password in your Wallet.

Click **No** if you do not want the user name and password to be stored for the moment. The next time you log on to the application, AccessAgent displays the same dialog box for confirmation.

Click **Never** if you do not want your user name and password to be stored for this application. The next time you log on to the application, AccessAgent no longer displays the dialog box for confirmation.

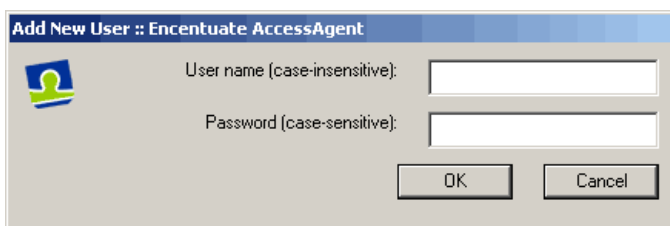
## Adding new users to authentication services

Use AccessAgent to store several user names and passwords for one application. For such scenarios, AccessAgent prompts you to enter the user name whenever you log on to that application.

For example, Helpdesk officers may have two different user names for the same authentication service. Another example would be having two web-based mail accounts. In this case, you can add a new user name and password to the existing authentication service.

*To add a new user to an authentication service:*

- 1 In the Manage Wallet window, click on the authentication service from the list. Click **Add New User**.



Add New User window

- 2 Enter the user name and password.



*Passwords are case-sensitive unless otherwise stated.*

---

- 3 Click **OK**.

## Searching for credentials within Wallet Manager

Use the **Credential Search** field to find credential details within Wallet Manager. As you enter the credential in the field, entries that match the search item will be highlighted on the list.

# Deleting users from authentication services

*To delete a credential entry from the Wallet:*

- ❶ In the Manage Wallet window, click on the user name of an authentication service.
- ❷ Click **Delete**. The entry is removed from the list of authentication services in your Wallet.

Alternatively, you can right-click on the entry and select **Delete Credentials**.



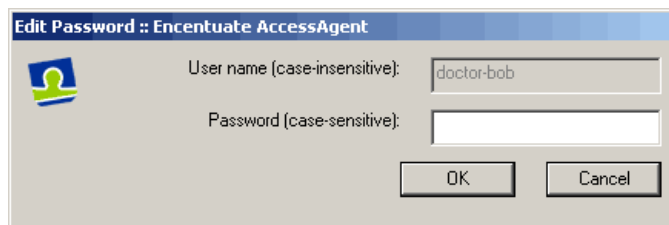
*AccessAgent will not ask you to confirm your deletion. Make sure you really want to delete the entry before clicking Delete.*

---

## Editing authentication service user names and passwords

*To edit an authentication service user name and password:*

- ❶ In the Manage Wallet window, click on the user name of an authentication service.
- ❷ Click **Edit Password** or right-click on the user name and select **Edit Password**.



Edit Password window

- ❸ Enter the new Password.
- ❹ Click **OK** to confirm the change.

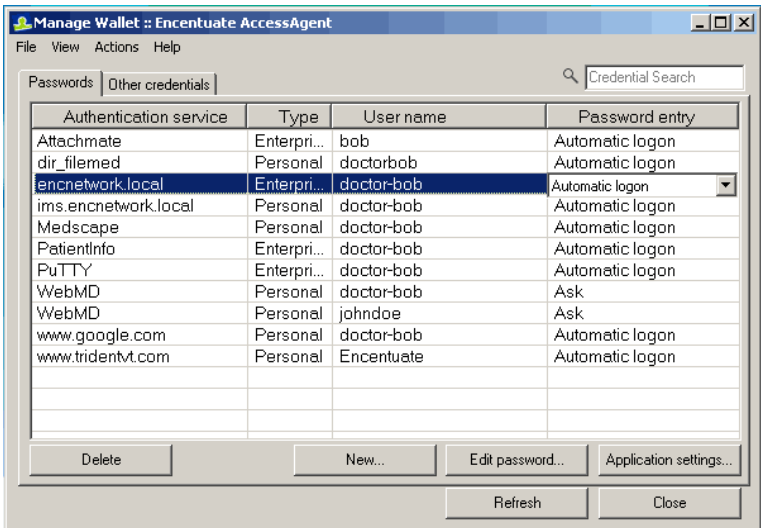
# Managing multiple applications for authentication services

Use the Application Settings option to manage the two applications as separate entities. A user can use several different applications to open one password-protected account. For example, a user has an e-mail account that can be accessed from either Outlook or a web-based e-mail application.

## Editing application settings

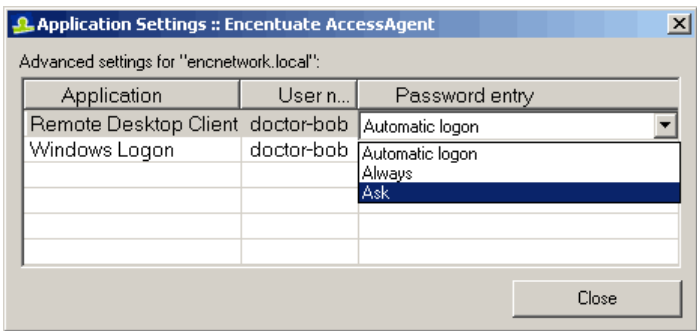
*To edit application settings:*

- 1 Click on the authentication service.



Wallet Manager

- 2 Click **Application Settings**. You can also right-click on the entry and select **Edit application settings**.



Advanced Settings window

- 3 In the **Password Entry** column, provide any necessary changes.




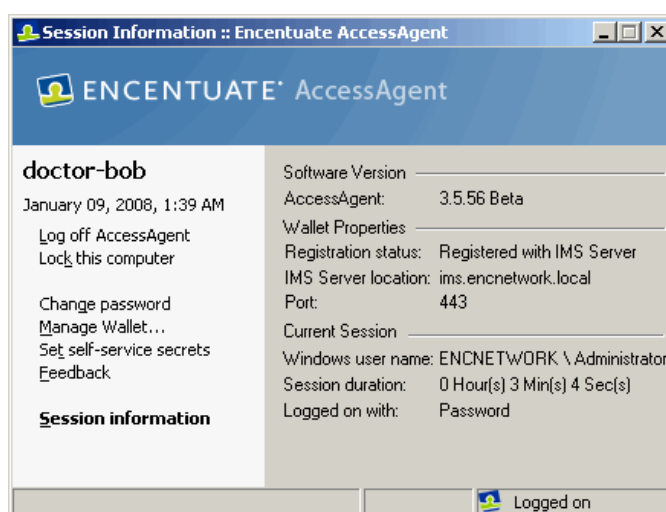
- 4 Click **Close** to confirm the changes.

# Changing Encentuate passwords


To ensure your Encentuate password is not compromised, your organization may schedule compulsory password changes. You can also change your password for the Wallet as often as needed by your organization.

*To change your Encentuate password:*

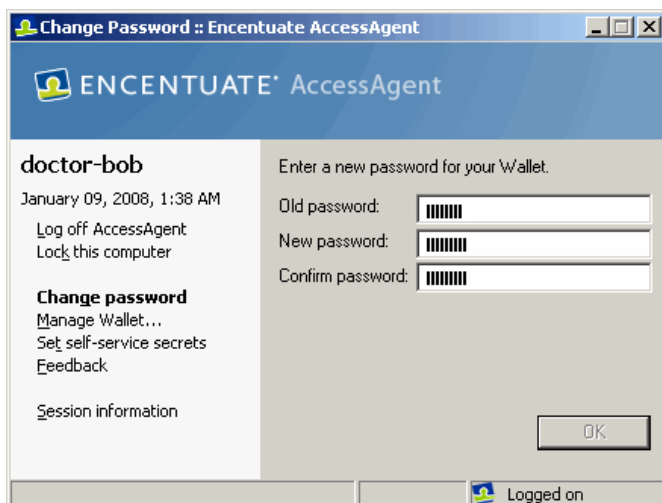
- 1 In the notification area, double-click on the AccessAgent icon . The Session information window is displayed.



Session information

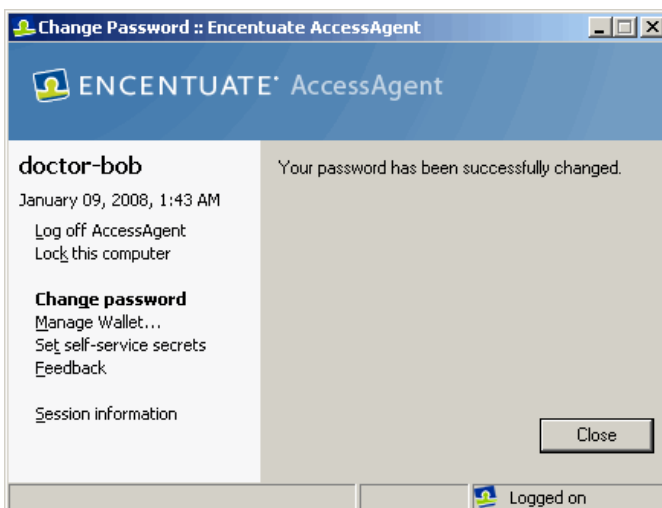
Alternatively, you can right-click on the AccessAgent icon  and select **Change password** from the context menu.

- 2 Click **Change password**.
- 3 Enter your **Old password**.
- 4 Enter your **New password**. The new password must match the specified requirements. Enter the new password again in the **Confirm password** field. Click **Next**.



Enter old and new passwords

- 5 Click **OK**. AccessAgent notifies you if the password change is successful.



Change password successful

- 6 Click **Close** to return to your desktop.

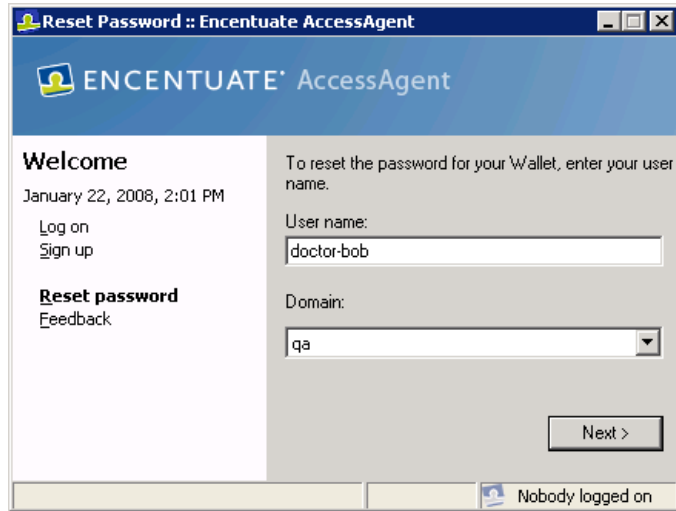
## Resetting Encentuate passwords (AccessAgent)

Use AccessAgent to reset an Encentuate password, usually when it has been forgotten.

The Helpdesk or Administrator cannot supply you with a new password. You need an authorization code to reset your Encentuate password.

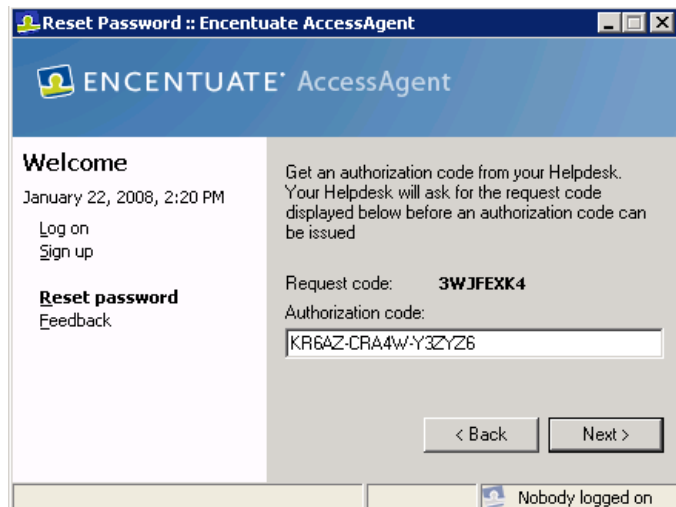
To reset your *Encentuate* password (without IMS connectivity):

- 1 In the AccessAgent navigation panel, click **Reset password**.



Enter user name

- 2 Enter your user name and click **Next**.
- 3 AccessAgent displays a dialog box, indicating that there is no IMS connectivity. You are now creating a temporary password on this computer so that you can still use AccessAgent. Click **OK**.
- 4 Contact Helpdesk for an authorization code. You need to supply a request code, which is displayed in your AccessAgent window.



Enter authorization code

- 5 Enter your authorization code and click **Next**.

Enter secret answer

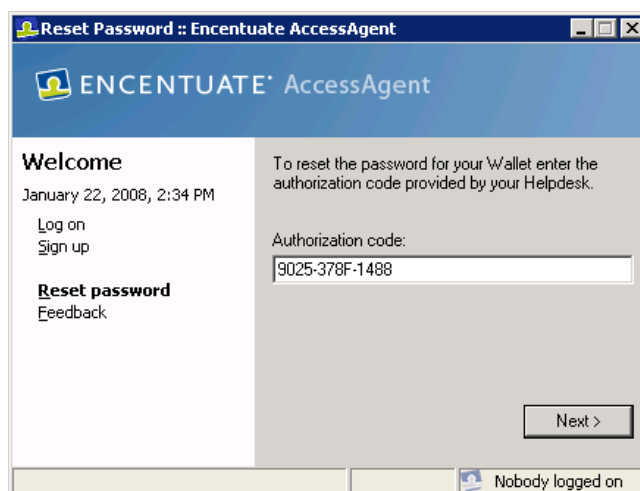
- 6 Enter the answer to the secret question and click **Next**.

Enter new password

- 7 Enter the new password. The new password must match the specified requirements. Enter the new password again in the **Confirm password** field.
- 8 Click **Finish**. The system displays a dialog box if the new password has been set successfully. Click **OK**.

*To reset your Encentuate password (with IMS connectivity):*

- 1 In the AccessAgent navigation panel, click **Reset password**.
- 2 Contact Helpdesk for an authorization code.



Enter new authorization code

- ③ Enter your authorization code and click **Next**.
- ④ Enter the answer to the secret question and click **Next**.
- ⑤ Enter your New password. The new password must match the specified requirement. Enter the new password again in the **Confirm password** field.
- ⑥ Click **Finish**. The system displays a dialog box if the new password has been set successfully. Click **OK**.



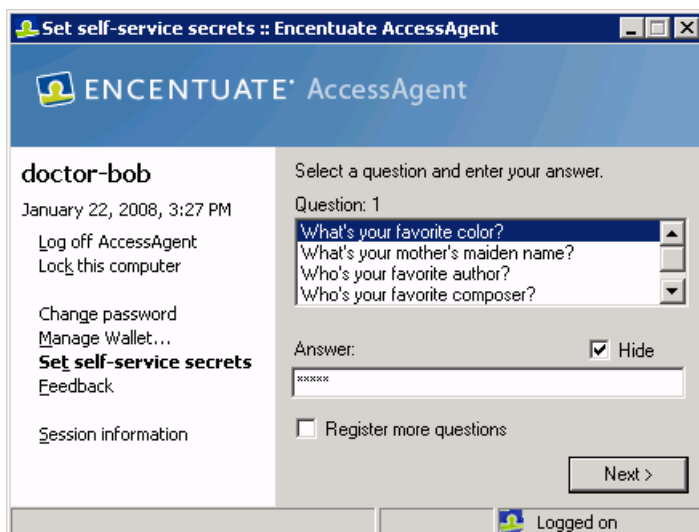
*Users can also reset their passwords without calling Helpdesk by answering two or more secret questions if self-service password reset is enabled.*

## Resetting self-service secrets (AccessAgent)

Use AccessAgent to reset or update secret questions and secret answers, including specify additional secret questions and secrets answers.

**To reset your secrets:**

- ① In the AccessAgent navigation panel, click **Set self-service secrets**.
- ② Select a new secret question from the drop-down list.

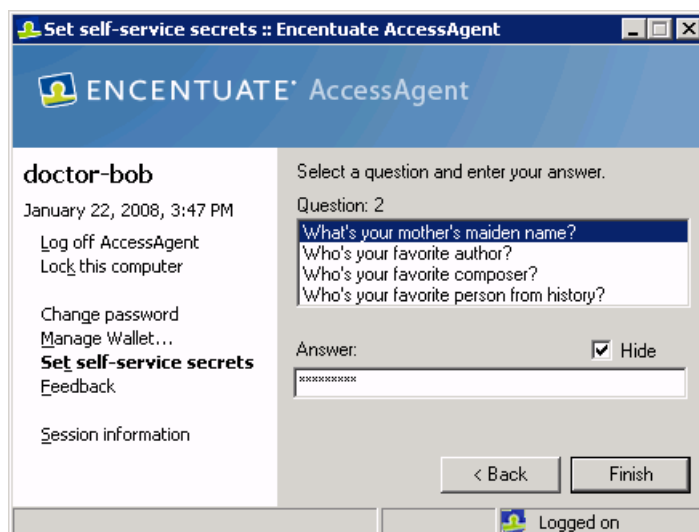


Resetting self-service secrets (first question)

- 3 Enter the secret answer.

Mark **Hide** if you do not want the answer to be visible. To register more questions, mark **Register more questions**.

- 4 Click **Next**.



Resetting self-service secrets (second question)

- 5 Select another secret question from the drop-down list and enter the corresponding secret answer.
- 6 Click **Next**.

If you chose to register more questions, you will be required to select another secret question and enter the corresponding secret answer. Click **Finish**.

If you chose not to register more questions, the AccessAgent panel will close and your new secret(s) will be saved.

## Bypassing strong authentication

You can log on to AccessAgent without your second factor authentication device (e.g., USB Key, RFID Card, or Active Proximity Badge) temporarily. You will need an authorization code from your Helpdesk.



*Your temporary access will expire when you receive a new second factor authentication device, or when the temporary access validity period ends.*

---

An authorization code is an alphanumeric code required to perform administrative functions and generated by the Helpdesk officer.

**To log on to AccessAgent without a second factor authentication device:**

- ❶ Turn on the computer.
- ❷ Press **Ctrl+Alt+Del** to log on, or click **Log on** from the AccessAgent navigation panel.
- ❸ Enter your user name and password.
- ❹ Contact Helpdesk for an authorization code.



*If you do not have Internet connectivity, you may see a request code in the AccessAgent window. Supply Helpdesk with this code to have an authorization code generated.*

---

- ❺ Enter your authorization code and click **Next**. You are now logged on.



*If there is IMS connectivity and self-service bypass is enabled, a user can bypass strong authentication by answering two or more secret questions.*

---

## Registering second factor authentication devices after signup

In some cases, a second factor authentication device only becomes available after sign up, so you would need to register the device with the IMS Server and associate it with your user name and password.

You also need to go through the same registration process if you have received a replacement second factor authentication device.

You need an authorization code to register an Active Proximity Badge.

**To register a second factor device:**

- ❶ Present or tap the device you want to register.
- ❷ If you are registering an Active Proximity Badge, select the Badge you want to register by clicking on its number.



*There may be several badges within range. Select the one that you are authorized to register. The badge ID is printed on the back of your Active Proximity Badge.*

---

- ❸ Click **Register**.
- ❹ AccessAgent displays a dialog box and verifies if you already have an Encentuate user name and password. Click **Yes**.
- ❺ Contact Helpdesk for an authorization code.
- ❻ Enter your authorization code and click **Next**.
- ❼ Enter your Encentuate password.
- ❽ Click **Finish**.

## Using AccessAssistant

Encentuate AccessAssistant is the web-based interface used to provide password self-help. Use AccessAssistant to obtain the latest credentials to log on to their applications. If AccessAgent cannot be used, such as if users need to access enterprise applications through SSL VPN from home computers or cyber cafes, the user can use AccessAssistant to retrieve passwords. AccessAssistant can also automatically log on to web-based enterprise applications.

The Web automatic sign-on feature allows users to log on to enterprise Web applications by clicking on links from AccessAssistant, Web Workplace, or enterprise portals, without entering the passwords for individual applications.

Users only need to remember the Encentuate password to log on to all applications. Combined with the reverse proxy feature, Web automatic sign-on can support a very large variety of Web applications.

AccessAssistant requires users to log on with at least the Encentuate password. If the Encentuate password is set up to synchronize with the Windows password, users can also use their Windows passwords to log on.



Once logged on, you can also use the following features of AccessAssistant:

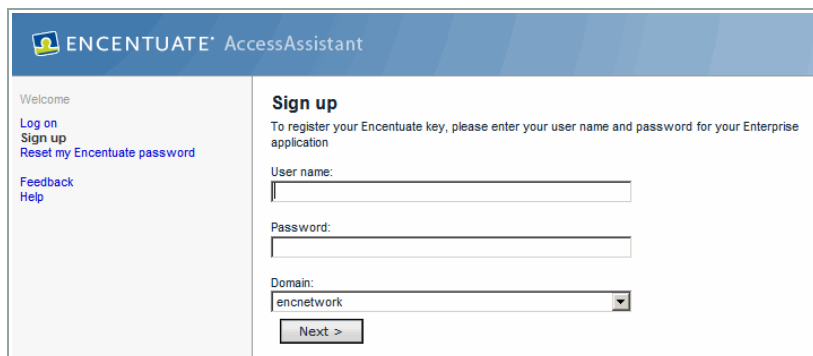
- Web automatic sign-on
- Reverse proxy
- User sign-up
- Manage application credentials (only applications that have AccessProfiles for Web automatic sign-on are listed.)
- Reset secrets
- Reset Encentuate password
- Modify user profile
- Optional two-factor authentication
- Synchronize Wallets, AccessProfiles, and policies

## Signing up from AccessAssistant

When you sign up, you must have an enterprise identity - a user name by which you are known in your organization. Your enterprise identity could be your email address, your Active Directory user name, your SAP user name, etc. Encentuate takes your enterprise identity and uses it to label your Encentuate Wallet.

*To sign up using AccessAssistant:*

- ❶ In the AccessAssistant left navigation panel, click **Sign up**.
- ❷ Enter your Windows user name and password. This is the user name and password you normally use to log on to your computer every day up to this point.

The screenshot shows the 'ENCENTUATE AccessAssistant' web interface. On the left is a navigation menu with links: 'Welcome', 'Log on', 'Sign up' (highlighted in blue), 'Reset my Encentuate password', 'Feedback', and 'Help'. The main content area is titled 'Sign up' and contains the instruction: 'To register your Encentuate key, please enter your user name and password for your Enterprise application'. Below this are three input fields: 'User name:', 'Password:', and 'Domain:'. The 'Domain:' field has a dropdown menu currently showing 'encnetwork'. At the bottom of the form is a 'Next >' button.

Signing up from AccessAssistant

- ❸ Click **Next**.

Selecting a secret question from AccessAssistant

- 4 Select a secret question. The answer to this question must be at least three characters long.

If you do not want the answers displayed, mark **Hide answer**.

- 5 Click **Finish**. If signup is successful, you will see a notification on the right panel.

Signup complete

## Logging on using AccessAssistant

When you are logged on, you have full access to all the application user names and passwords stored in your Wallet.

*To log on to your Wallet using AccessAssistant:*

- 1 In the AccessAssistant left navigation panel, click **Log on**.

Logging on from AccessAssistant

- ② Enter your Encentuate user name and password.
- ③ Click **Next**. You now have access to AccessAssistant features.

## Logging on to applications from AccessAssistant

Once logged on, the enterprise and personal web applications available for you are listed in the right panel of the AccessAssistant page. To log on to an application on the list, click on the application name. A new browser page opens with the requested application, automatic sign-on having been performed.

<input type="checkbox"/>	Application	Type	User name	
<input type="checkbox"/>	Attachmate	Personal	doctor-bob	<a href="#">Get password &gt;&gt;</a>
<input type="checkbox"/>	Google	Enterprise	jane smith	<a href="#">Get password &gt;&gt;</a>

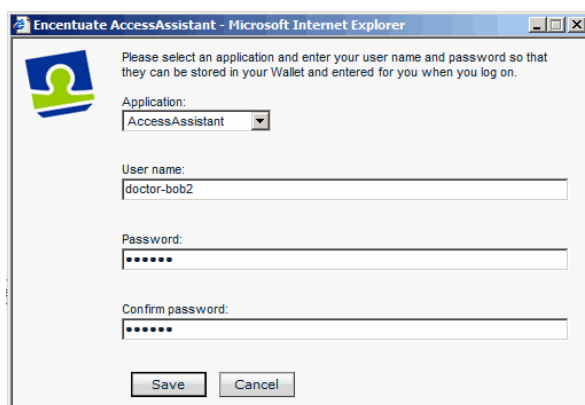
Logging on to applications from AccessAssistant

## Adding accounts to applications (AccessAssistant)

If the application to log on is not in your Wallet, it means that your user name and password for that application was not captured by AccessAssistant. Click the **Add** button in the Manage logon accounts page to add one or more user name(s) for the application.

### *To add an account to an application:*

- 1 Click **Add** in the Manage logon accounts page. A new window appears, asking you to add the application details.
- 2 Select an application from the drop-down list.

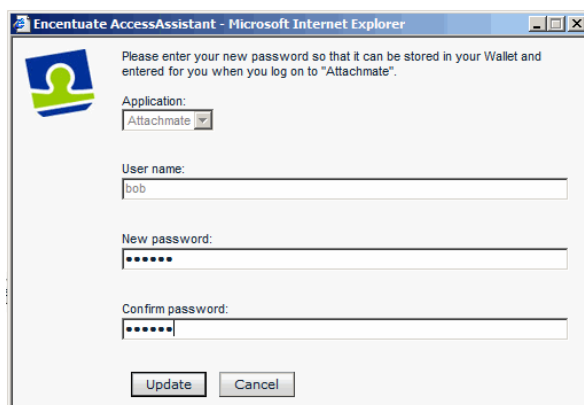


Adding application accounts from AccessAssistant

- 3 Enter your user name and password.
- 4 Enter your password again to confirm.
- 5 Click **Save**.

## Editing application passwords (AccessAssistant)

You can change an application's password, by clicking **Edit password** next to the corresponding user name in **My Wallet** page.



Editing application passwords from AccessAssistant

### *To edit an application's password:*

- 1 In the Edit password window, enter the new password.

- ❷ Enter the new password again to confirm.
- ❸ Click **Save**.

## Deleting accounts from applications (AccessAssistant)

To delete an application from your Wallet, mark the checkbox next to the corresponding application, then click **Delete**.

The screenshot shows the ENCENTUATE AccessAssistant web interface. On the left is a sidebar with links: Log off, My Wallet, Manage AccessProfiles, Synchronize system data with IMS Server, Reset my secrets, Feedback, and Help. The main content area has a header 'Select an option for getting application password:' with two radio buttons: 'Display password on the browser' (selected) and 'Copy password to the clipboard so that I can paste it in the password field'. Below this is a table with columns 'Application', 'Type', and 'User name'. The table lists 'Attachmate' (Personal, doctor-bob) and 'Google' (Enterprise, jane smith). Each row has a 'Get password >>' link. At the bottom are buttons for 'Add >', 'Delete', and 'Edit password >'.

Deleting application accounts from AccessAssistant

## Retrieving passwords (AccessAssistant)

*To retrieve your application password:*

- ❶ You can:
  - Display the password on the browser, or
  - Copy the password to the clipboard and paste it in the **password** field.
- ❷ Mark the appropriate checkbox to select the password retrieval option.

The screenshot shows the ENCENTUATE AccessAssistant web interface. The 'Display password on the browser' radio button is selected. A timer at the top indicates 'Your password will be cleared in 55 seconds.' The table below shows 'Attachmate' (Personal, bob) with a checkbox checked and a 'password' field with a '<<' button. The 'Google' (Enterprise, jane smith) row has its checkbox unchecked and a 'Get password >>' link.

Retrieving application passwords from AccessAssistant (1/2)

encnetwork.localdoctor-bob

Log off  
My Wallet  
Manage AccessProfiles  
Synchronize system data with IMS Server  
Reset my secrets  
Feedback  
Help

Your password will be cleared in 46 seconds.

Application	Type	User name
<input checked="" type="checkbox"/> Attachmate	Personal	doctor-bob

Password copied to clipboard. <<

Retrieving application passwords from AccessAssistant (2/2)



If you select **Display password on the browser**, the password will be displayed to you and anyone who can see your monitor. Make sure you have some privacy before displaying the password.

## Optional two-factor authentication

If two-factor authentication is turned on, supply one of the following to log on, in addition to your Encentuate password:

- Authorization code issued by Helpdesk
- MAC, which can be sent to user via mobile phone or email.
- One-time Password (OTP) provided by an OTP token (e.g., VASCO Digipass).

## Resetting secrets (AccessAssistant)

AccessAssistant offers a host of self-service capabilities to the users, such as the ability to reset their secret questions and secret answers. Instead of calling Helpdesk for an authorization code, the self-service feature allows users to reset their Encentuate passwords by providing a subset of their previously specified secret questions.

**To reset your secrets:**

- ❶ In the AccessAssistant left navigation panel, click **Reset my secrets**.
- ❷ Select a new secret question from the drop-down list.
- ❸ Enter the secret answer. Mark **Hide** if you do not want the answer to be visible.
- ❹ You can specify an optional second secret question and secret answer.

The screenshot shows the ENCENTUATE AccessAssistant web interface. On the left is a navigation menu with links: Log off, My Wallet, Manage AccessProfiles, Synchronize system data with IMS Server, Reset my secrets (highlighted), Feedback, and Help. The main content area has a header with the ENCENTUATE logo and 'AccessAssistant'. Below the header, it says 'encnetwork.local\doctor-bob'. The main section contains instructions: 'Select 3 different questions and enter your secret answers that you are not likely to forget. In case you forget your password, you will need to use these secret answers to help you retrieve your Wallet contents.' It then lists requirements: 'Your answer must meet these requirements: 1. At least 3 characters long.' There are three question sets. Each set has a question dropdown (e.g., 'What's your mother's maiden name?'), an answer input field with a password mask (dots), and a 'Hide answer' checkbox. At the bottom is a 'Reset' button.

Resetting secrets from AccessAssistant

- 5 Click **Reset** to save the new secret question(s) and secret answer(s).

If reset is successful, a notification appears in the right panel.

The screenshot shows the ENCENTUATE AccessAssistant web interface after a successful reset. The left navigation menu is the same. The main content area now displays a large blue box with the text 'Reset secret complete' and 'You have successfully reset your secrets.' The 'Reset my secrets' link in the navigation menu is still highlighted.

Resetting secret complete

## Resetting Encentuate passwords (AccessAssistant)

*To reset your Encentuate password:*

- 1 In the AccessAssistant left navigation panel, click **Reset my Encentuate password**.

Resetting Encentuate passwords from AccessAssistant

- 2 Enter your Encentuate user name.
- 3 Click **Next**.

Specifying secrets for resetting Encentuate passwords

- 4 Enter the secret answer. You must enter both secret answers.
- 5 Click **Next**.
- 6 Enter your new password. The new password must meet the requirements listed on the right panel.
- 7 Enter the new password again to confirm.



Entering the Encentuate password

- 8 Click **Next**. If password reset is successful, you will see a notification in the right panel.

Reset password complete

If you cannot remember one of your secret answers, you can still reset your Encentuate password with an authorization code issued by Helpdesk.

**To reset your Encentuate password without a secret answer:**

- 1 In the AccessAssistant left navigation panel, click **Reset my Encentuate password**.
- 2 Enter your Encentuate user name.
- 3 Click **Next**
- 4 Enter both secret answers. In case you forgot the secret answers, click the link in the instruction just above the **Next** button which says:

If you do not remember your answers, please click [here](#).

This will prompt you for an authorization code.

Resetting password by entering an authorization code

- 5 Contact Helpdesk to request for an authorization code. The number to contact should be available on your AccessAssistant page.
- 6 Enter the authorization code. The authorization code is not case-sensitive.
- 7 Click **Next**.

Selecting the secret question and entering the answer

- 8 Enter one secret answer that you provided during signup.
- 9 Click **Next**.

Entering the new password

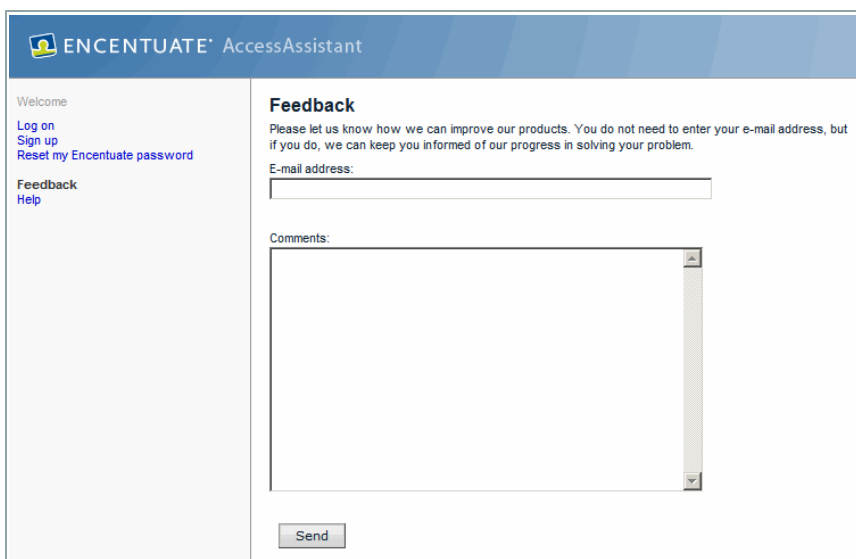
- 10 Enter a new password.

- 11 Enter the new password again to confirm.
- 12 Click **Next**. If reset password is successful, you will see a notification in the right panel.

## Sending feedback

You can send feedback on AccessAssistant to the Encentuate team by clicking **Feedback** in the AccessAssistant left navigation panel.

Enter your email address and comments, then click **Send**.

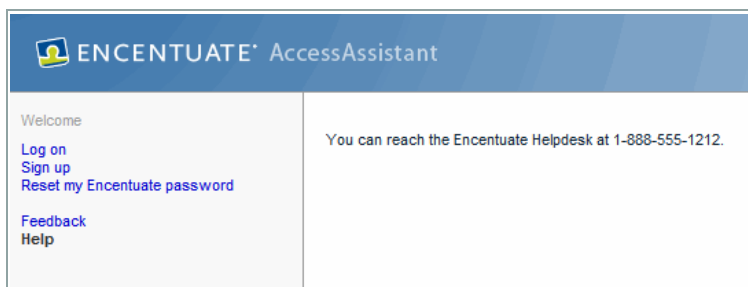


The screenshot shows the 'Feedback' page of the Encentuate AccessAssistant interface. The header bar is blue with the Encentuate logo and the text 'ENCENTUATE AccessAssistant'. On the left, a navigation panel lists 'Welcome', 'Log on', 'Sign up', 'Reset my Encentuate password', 'Feedback' (highlighted), and 'Help'. The main content area is titled 'Feedback' and contains the text: 'Please let us know how we can improve our products. You do not need to enter your e-mail address, but if you do, we can keep you informed of our progress in solving your problem.' Below this text are two input fields: 'E-mail address:' and 'Comments:'. The 'Comments:' field is a large text area with a vertical scrollbar. At the bottom right of the form is a 'Send' button.

Sending feedback on AccessAssistant

## Getting help

If you need help on any of the features of AccessAssistant, you can click **Help** in the AccessAssistant left navigation panel.



The screenshot shows the 'Help' page of the Encentuate AccessAssistant interface. The header bar is blue with the Encentuate logo and the text 'ENCENTUATE AccessAssistant'. On the left, a navigation panel lists 'Welcome', 'Log on', 'Sign up', 'Reset my Encentuate password', 'Feedback', and 'Help' (highlighted). The main content area displays the text: 'You can reach the Encentuate Helpdesk at 1-888-555-1212.'

Contacting Helpdesk



# Troubleshooting

---

This section discusses the different issues that you may encounter while using the Encentuate Wallet, an Encentuate authentication factor, or Encentuate AccessAgent, and their possible solutions. Try these solutions before you contact your Helpdesk officer.

- [AccessAgent-related problems](#)
- [USB Key-related problems](#)
- [RFID card-related problems](#)
- [Active Proximity Badge-related problems](#)

## AccessAgent-related problems

This section discusses problems that you may encounter when installing Encentuate AccessAgent.

### Unable to install AccessAgent

Refer to the following checklist. Either of these may be preventing you from installing AccessAgent:

- **Not using an Administrator account**

You cannot install AccessAgent without Windows Administrator privileges. If your Windows user account is not an Administrator account, contact your Helpdesk officer.

- **Not enough free disk space**

To install AccessAgent, you must have at least 32 MB of free hard disk space. If your computer does not have the required free disk space, free up some space by emptying your Recycle Bin and deleting unwanted files.

- **Installation files are corrupted**

If you downloaded the file from the Internet, it may not have completed successfully. You may want to download the file again.

The file available on the Internet may be corrupted. For such cases, contact your Helpdesk officer.

- **No connection to the IMS Server**

Refer to [Installer cannot find IMS Server](#)

- **Conflicts with another application**

If you see a message that says, "AccessAgent's setup detected a conflict with an application and it is recommended you uninstall the application", exit from the AccessAgent setup and uninstall the application that is causing the conflict. Make sure that you no longer need the application before uninstalling it. Once you are done, re-install the application. If you ignore the prompt and continue with the installation, AccessAgent may not work properly.

- **A module could not be registered**

If you see a message that says, "AccessAgent encountered a problem while registering a module (Error 1904), click Ignore to continue the installation". This is a documented Microsoft Windows problem and is not critical. If the problem persists, uninstall AccessAgent and re-install AccessAgent. If the problem persists, contact your Helpdesk officer.

## Network connection problems

Refer to the following checklist. Either of these may be preventing you from connecting to the network successfully:

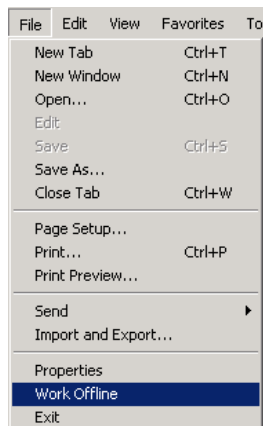
- **No network connection**

A network connection is required to install AccessAgent, to sign up, or to change your Encentuate password. If a network connection is not detected, you will be prompted.

Try to confirm that you have the correct network settings before you contact your Helpdesk officer.

- **Internet Explorer is set to offline**

If you see a network connection message, it may be because your Internet Explorer is set to offline mode. You can check this by going to the File menu in Internet Explorer. **Work Offline** should not be checked.



Internet Explorer File Menu - Work offline

## Installer cannot find IMS Server

The installer cannot locate the IMS Server because:

- **The server information is incorrect.**

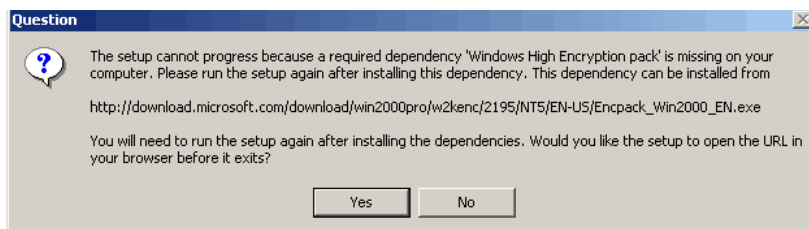
The installer tries to connect to the IMS Server automatically during the installation. If a connection is not established, you will be asked to enter the location of the IMS Server. If the IMS Server cannot be located, a message is displayed.

Check if the information you entered is correct and try again.

- **A network connection cannot be detected. If neither solution works, contact your Helpdesk officer.**

## No encryption pack

If you are installing AccessAgent on Windows 2000, you must have Enhanced Cryptographic Service Provider (CSP) installed on your computer. This is to ensure the security of the Wallet's contents.



No enhanced CSP

To check if you have Enhanced CSP, go to **Help > About Internet Explorer** in Internet Explorer. If Enhanced CSP is installed it will read *Cipher Strength: 128-bit*.



Checking the cipher strength

You can download Enhanced CSP from: <http://www.microsoft.com/windows2000/downloads/recommended/encryption/>.

## The password is not accepted

If your password is not accepted, it may be because your password was not entered correctly (e.g., incorrectly entered or incorrect case).

Before you re-enter your password, check the **Caps Lock** key and make sure the characters are entered in the correct case.

Your Wallet will be locked after five (or more, depending on your organization's preference) unsuccessful attempts to log on using an incorrect Encentuate password. If this happens, contact your Helpdesk officer.

## The authorization code is not accepted

If your authorization code is not accepted, it could be because:

- You did not enter the correct authorization code.

Make sure that the letters and numbers in the authorization code is entered in the correct order. The authorization code is **not** case-sensitive, and you can omit the hyphens.

- You did not receive the correct authorization code.



The wrong authorization code may have been communicated to you, or it may be incomplete (some characters missing). Contact your Helpdesk officer to verify the authorization code.

## Change password problems

### Entries do not match

If you are trying to change your password and your entries for **New password** and **Confirm Password** do not match, you will be prompted that the entries do not match. Re-enter the password in both **New Password** and **Confirm Password** fields. Make sure that both entries are the same.

### Password length

If you are trying to change your password and your new password is shorter or longer than the required length, you will be prompted to enter a password that follows your organization's password conventions.

The maximum and minimum length of your password is determined by your organization. Review the password length requirements.

### No network connection

You will be prompted if a network connection is not detected while you are trying to change your password. Check your network connection and then try again.

## I cannot remember my Windows user name and password

If you cannot remember your Windows user name and password, do the following:

- 1 Once you are logged on to Windows and AccessAgent has started, click **Ctrl-Alt-Del**. The Windows Security dialog box is displayed. Click **Change Password**.



Windows security

- ② Enter your password when prompted.



Enter password

- ③ In the next dialog box, your old password will be automatically entered for you. Enter a new password and remember this password. Click **OK** and the new Windows password will be stored in your Wallet.

## Unable to sign up for an Encentuate Wallet

Before you sign up for an Encentuate Wallet, enter your Windows user name and password to store them in the Wallet. The user name and password are verified with Windows. If they do not match, you will get an error message.

Check if you have entered the correct user name and password. Also, check the **Caps Lock** key is not active, and make sure letters are entered in the correct case. If the problem persists, contact your Helpdesk officer.

# The temporary Wallet's validity period has expired

If you are given a temporary access to your Wallet, the Wallet is only valid for a predefined time. Once the validity of the temporary Wallet expires, it can no longer be used. Contact your Helpdesk officer and obtain a new authorization code to gain temporary access.

# The Encentuate Wallet has been locked

Your Encentuate Wallet will be locked after five (5) unsuccessful attempts to log on using an incorrect password. If this happens, contact your Helpdesk officer to obtain an authorization code to unlock your Wallet.

If you are using a USB Key, you can temporarily log on without using your USB Key, by obtaining an authorization code from Helpdesk officer. Remove the USB Key from the computer, and log on to AccessAgent.

You must return the USB Key to your Helpdesk officer, and the Helpdesk officer will issue another USB Key for you.

## USB Key-related problems

This section discusses problems that relate to an Encentuate USB Key.

### Unable to unlock the computer with a USB Key

If you are trying to unlock your computer and you are prompted that your password could not be validated, remove and re-insert your Key from the USB port.

If the problem persists, unlock the computer using your Windows user name and password. Select **Go to Windows to unlock** in the navigation panel of the Unlock This Computer window.

If the problem persists, contact your Helpdesk officer.

### Lost Encentuate USB Key

If you have lost your Encentuate USB Key, you can still use the Wallet stored in the server. You can then register a new USB Key with the IMS Server and associate it with your Wallet. For more information, see [Signing up with your USB Key](#). As a temporary solution, you can also log on without your USB Key.

# Unable to remember the password

If you have forgotten the Encentuate password, you need to reset it. Contact your Helpdesk officer to receive an authorization code for password reset. You also need to return your USB Key to Helpdesk for resetting. For more information, see [Resetting Encentuate passwords \(AccessAgent\)](#).

# Unable to log on to the Wallet

There can be several reasons why you cannot log on to your Wallet.

- **You did not enter the correct password.**

Before you re-enter your password, check that the **Caps Lock** key is not active and make sure letters are entered in the correct case.

- **Your Encentuate USB Key is damaged or corrupted.**

If your Encentuate USB Key is damaged or corrupted, contact your Helpdesk officer to get a replacement.

- **Your Encentuate USB Key could not be detected.**

There may be a time-out while trying to access, validate, or detect your USB Key. Remove and re-insert your USB Key from the USB port. If the problem persists, restart your computer. If the problem persists, contact your Helpdesk officer.

# Unable to register a USB Key

## USB Key is already registered

If your Encentuate USB Key is already registered with the IMS Server, you will be prompted. Your USB Key has probably been used by another user, but has not been revoked from the IMS Server. Return the USB Key to your Helpdesk officer and request for a new USB Key.

## The USB Key has been revoked

If you lose your USB Key or report it as missing, your Helpdesk officer will revoke it. If you find the USB Key and try to use it, you will see a message that informs you that it has been revoked.

To use a revoked USB Key, obtain an authorization code from your Helpdesk officer, and then register the USB Key again to associate it with your Wallet.

# RFID card-related problems

This section discusses problems that relate to an Encentuate RFID card and reader.

## Lost Encentuate RFID card

If you have lost your Encentuate RFID card, you can still use the Wallet stored in the server. You can then register a new RFID card with the IMS Server and associate it with your Wallet. For more information, see [Signing up with your RFID card](#). As a temporary solution, you can also log on without your RFID card.

## Unable to remember the password

If you have forgotten your password for your Encentuate Wallet, you need to reset your Encentuate password. Contact your Helpdesk officer for an authorization code. For more information, see [Resetting Encentuate passwords \(AccessAgent\)](#).

## Unable to log on to the Wallet

There can be several reasons why you cannot log on to your Wallet.

- You did not enter the correct password.

Before you re-enter your password, check that the **Caps Lock** key is not active and make sure letters are entered in the correct case.

- Your Encentuate RFID card or reader is damaged or corrupted.

If your Encentuate RFID card is damaged or corrupted, contact your Helpdesk officer to get a replacement.

- Your Encentuate RFID card could not be detected.

There may be a time-out while trying to detect your RFID card. Try to tap the RFID card on the reader again. If the problem persists, restart your computer. If the problem persists, contact your Helpdesk officer for help.

## Unable to register the RFID card

### RFID card is already registered

If your Encentuate RFID card is already registered with the IMS Server, you will be prompted. Your RFID card has probably been used by another user, but has not been revoked from the IMS Server. Return the RFID card to your Helpdesk officer and request for a new RFID card.

## RFID card has been revoked

If you lose your second authentication factor or report it as missing, your Helpdesk officer will revoke it. If you find the RFID card and try to use it, you will see a message that informs you that it has been revoked.

To use a revoked RFID card, obtain an authorization code from your Helpdesk officer, and then register the RFID card again to associate it with your Wallet.

# Active Proximity Badge-related problems

This section discusses problems that relate to an Encentuate Active Proximity Badge and reader.

## Lost Encentuate Active Proximity Badge

If you have lost your Encentuate Active Proximity Badge, you can still use the Wallet stored in the server. You can then register a new Active Proximity Badge with the IMS Server and associate it with your Wallet.

See [Signing up with your active RFID card](#) to find out how. As a temporary solution, you can also log on without your Active Proximity Badge.

## Unable to remember the password

If you have forgotten your password for your Encentuate Wallet, reset your Encentuate password. Contact your Helpdesk officer for an authorization code. For more information, see [Resetting Encentuate passwords \(AccessAgent\)](#).

## Unable to log on to the Wallet

There can be several reasons why you cannot log on to your Wallet.

- **Entering an incorrect password.**

Before you re-enter your password, check that the **Caps Lock** key is not active and make sure letters are entered in the correct case.

- **The Encentuate Active Proximity Badge or reader is damaged or corrupted.**

If your Encentuate Active Proximity Badge is damaged or corrupted, contact your Helpdesk officer to get a replacement.

■ **Your Encentuate Active Proximity Badge could not be detected.**

There may be a time-out while trying to detect your Active Proximity Badge, or the card has been switched on for nine hours—after which automatically switches off. Try to switch the badge off and on. If the problem persists, restart your computer. If the problem persists, contact your Helpdesk officer.

## Unable to register Active Proximity Badge

### Active Proximity Badge is already registered

If your Encentuate Active Proximity Badge is already registered with the IMS Server, you will be prompted. Your Active Proximity Badge has probably been used by another user, but has not been revoked from the IMS Server. Return the Active Proximity Badge to your Helpdesk officer and request for a new RFID card.

### Active Proximity Card has been revoked

If you lose your Active Proximity Badge or report it as missing, your Helpdesk officer will revoke it. If you find the Active Proximity Badge and try to use it, you will see a message that informs you that it has been revoked.

To use a revoked Active Proximity Badge, obtain an authorization code from your Helpdesk officer, and then register the Active Proximity Badge again to associate it with your Wallet.

## Active Proximity Badge cannot be detected

The placement of the reader and badge can be the cause for the fluctuation of the signal. The reader and badge should be positioned at the same level. For example, if the reader is mounted on the monitor, then the badge should be around the upper part of the body.

The distance is not the issue, but rather the possibility for other things to affect the radio frequency signal, such as the desk, the body, the keyboard, and others. All of these things can have an effect on the strength of the signal. Even a user's arm passing in front of the reader can cause the signal to drop slightly.

You can review the badge positioning demo at the following URL: <http://www.ensuretech.com/support/documentation/movies/lockpositionlowres.mpg>





# Glossary and Abbreviations

---

## **AccessAdmin**

The management console used by individuals with the Administrator Role and/or the Helpdesk Role to administer IMS Server, and to manage users and policies.

## **AccessAgent**

The client software that manages the user's identity, enabling sign-on/sign-off automation and authentication management.

## **AccessAssistant**

The web-based interface used to provide password self-help for users to obtain the latest credentials to logon to their applications.

## **AccessProfiles**

Short, structured XML files that enable single sign-on/sign-off automation for applications. AccessStudio can be used to generate AccessProfiles.

## **AccessStudio**

The interface used to create AccessProfiles required to support end-point automation, including single sign-on, single sign-off, and customizable audit tracking.

## **AD**

Microsoft Active Directory

## **Administrator role**

A role gives users the ability to use AccessAdmin to manage users, policies, and the IMS Server. The role is one of three Encentuate Predefined Roles within the Encentuate IAM system.

## **ADSI**

Active Directory Service Interfaces

## **agent-driven, server managed**

Encentuate's distributed SSO architecture where the AccessAgent provides personal identity management functions to the users, centrally managed through the Encentuate IMS Server. Also known as server-managed.

## **API**

Application Programming Interface

## **application**

In AccessStudio, it refers to the system that provides the user interface for reading/entering the authentication credentials.

## **application group**

A set of applications that share the same directory. In other words, a user can logon to any of the applications in the application group using the same user name.

## **application policy**

Collections of policies and attributes governing access to applications.

## **authentication**

Questions used to validate the identity of a user.

## **authentication factor**

The different devices, biometrics, or secrets required as credentials for validating digital identities (e.g., passwords, Encentuate USB Key, RFID, biometrics, and one-time password tokens).

## **authentication service**

Verifies the validity of an account; Applications authenticate against their own user store or against a corporate directory.

## **authorization code**

An alphanumeric code generated by an Encentuate Helpdesk user for administrative functions, such as password resets or authentication factors for the Wallet; may be used one or more times based on policy.

## **auto-capture**

A function that allows the system to remember user credentials (e.g., user names and passwords) for different applications. These credentials are captured as they are being used for the first time, and then stored and secured in the Encentuate Wallet for future use.

## **auto-inject**

A function that allows the system to enter user credentials automatically (such as user names and passwords) for different applications, via sign-on automation.

## **biometrics**

The identification of a user based on a physical characteristic of the user, such as a fingerprint, iris, face, voice or handwriting.

## **CA**

Certificate Authority

## **CLT**

Command Line Tool

## **CSN**

Card Serial Number (for Mifare RFID cards)

## **Common Symmetric Key (CSK)**

An encryption key that is encrypted using by public keys. It is used as a performance optimizer, and to share secrets to multiple entities with public keys.

## **conventional single sign-on**

Refers to web-based single sign-on systems and typically requires server-side integration, with a centralized architecture.

## **credentials**

Refer to user names, passwords, certificates, and other information for authentication. An authentication factor can serve as a credential. In Encentuate IAM, credentials are stored and secured in the Wallet.

## **DB**

Database

## **directory**

A structured repository of information on people and resources within an organization, facilitating management and communication.

## **directory services**

A directory of the names, profile information and machine addresses of every user and resource on the network. It is used to manage user accounts and network permissions. These use highly specialized databases that are typically hierarchical in design and provide fast lookups.

## **DLL**

Dynamic Link Library

## **DNS**

Domain Name Service

## **Encentuate**

To *enable* and *accentuate*, as it applies to security.

## **Encentuate password**

A password used to secure access to an Encentuate Wallet.

## **Encentuate USB Key**

Encentuate's customized token that combines the utility and capacity of Flash RAM, the security of a smart card, and the universal connectivity of Universal Serial Bus (USB). It is a portable and personalized device for storing user names, passwords, certificates, encryption keys, and other security credentials.

## **EnGINA**

Encentuate GINA, which replaces the Microsoft GINA. EnGINA provides a user interface that is tightly integrated with authentication factors and provide password resets and second factor bypass options.

## **Enterprise Access Security (EAS)**

A technology that enables enterprises to simplify, strengthen and track access to digital assets and physical infrastructure.

## **enterprise directory**

The master reference directory for the enterprise. In Encentuate IAM, each user registration is verified against the enterprise directory. The user name for the enterprise directory can be used as the user name for Encentuate.

## **Enterprise Single Sign-On (ESSO)**

A mechanism that allows users to log on to all applications deployed in the enterprise by entering a user ID and other credentials (such as a password). Many ESSO products use sign-on automation technologies to achieve SSO—users logon to the sign-on automation system and the system logs on the user to all other applications.

## **fortified password**

A fortified password is an application password that is automatically changed without human intervention. In Encentuate IAM, passwords might be fortified with Encentuate ActiveCodes.

## **Helpdesk role**

A role that gives its owner the ability to manage certain groups of Encentuate Users (e.g., perform password resets, issue authorization codes, and revoke access rights of users). This role is one of three Predefined Roles within the Encentuate IAM system.

## **identity wallet**

A secured data store for a user's access credentials and related information (including user IDs, passwords, certificates, encryption keys). The Wallet is an identity wallet.

## **knowledge-based authentication**

A method of authentication where questions are used to validate the identity of a user. This is an insecure method of authentication, so it is typically used in areas where it reveals information that is only useful with other information or authentication factors.

## **IMS Bridge**

IMS Service Modules that enable applications to use the Encentuate IMS Server as an authentication server. Examples include IMS Bridges that provide OTP and certificate-based authentication services for applications.

## **IMS Connector**

Add-ons to the IMS Server that enable the IMS Server to interface with other applications as a client, extending the capability of the IMS Server. Examples include IMS Connectors for password change.

## **IMS Server**

An integrated management system that provides a central point of secure access administration for an enterprise. It enables centralized management of user identities, AccessProfiles, authentication policies, provides loss management, certificate management and audit management for the enterprise.

## **Lock Computer**

An AccessAgent feature that allows you to lock your computer and prevent anyone from using it. Only you can unlock the computer.

## **Mobile Active Code (MAC)**

A one-time password that is randomly generated, event-based, and delivered via a secure second channel (e.g., SMS on mobile phones).

### **mobile authentication**

An authentication factor which allows mobile users to sign-on securely to corporate resources from anywhere on the network. In Encentuate IAM, it provides an optional authentication factor for the Encentuate Wallet and other enterprise applications. An example is sending an Encentuate ActiveCode to a mobile device through SMS (short messaging service).

## **One-Time Password (OTP)**

A one-use password generated for an authentication event (e.g., password reset), sometimes communicated between the client and the server via a secure channel (e.g., mobile phones).

### **password**

A sequence of characters used to determine that a user requesting access to a system is the appropriate user. The assumption is that only the authentic user will have the passwords to access their accounts.

### **password fortification**

The process of strengthening application passwords through regular password changes and stronger password requirements.

### **password reset**

Allows the user to reset the password of the Wallet, and will require an authorization code.

### **personal applications**

Windows and web-based applications that AccessAgent can store and enter credentials. Some enterprises may not allow the use of an Encentuate Key with personal applications. Password fortification also does not happen for personal applications.

Some examples of personal applications are web-based mail sites such as Yahoo! Mail and Hotmail, Internet banking sites, Amazon.com, chat or instant messaging programs and the like.

## **Personal Identification Number (PIN)**

A password, typically of digits, entered through a telephone keypad or automatic teller machine.

### **physicalization**

A technique in which a digital identity is attached to a physical device and cannot be replicated without replicating the physical device. An Encentuate USB Key supports this technique as it contains a smart card with on-board cryptographic and wallet caching capabilities. The smart card ensures that the Encentuate Wallet is protected.

### **policy**

Governs the operation of Encentuate IAM Enterprise, comprising of two (2) main sets: machine policies (managed through Windows GPO) and IMS-managed policies (managed through AccessAdmin).

### **predictive passwords**

Generated passwords that can change between a client and a server without communication between them. This change can be achieved by using cryptographic hash algorithms and an initial shared secret (or seed) between the client and the server.

### **private key**

An encryption/decryption key that is kept secret by its owner. It is one of a pair of two keys used for encryption and decryption in public key cryptography.

### **public key**

A public key is an encryption/decryption key that is publicly associated with its owner. It is one of a pair of two keys used for encryption and decryption in public key cryptography.

## public key cryptography

A coding system in which encryption and decryption are done with public and private keys, allowing users who don't know each other to send secure or verifiable messages.

## Radio Frequency Identification (RFID)

A wireless technology that transmits product serial numbers from tags to a scanner, without human intervention.

## RADIUS

Remote Authentication Dial-In User Service

## random ActiveCodes

Random passwords created and delivered through various second channels, including SMS (short messaging service).

## random passwords

Generated passwords used to increase authentication security between clients and servers. Random password change is the process of modifying access codes between a client and a server using a random sequence of characters. This change can only happen when the client and the server are sharing a secured session as the random sequence has to be communicated between the two parties. The new random password can then be used to re-establish a secured session the next time the client needs to access the server.

## RDP

Remote Desktop Protocol

## RDP Client

Another name for **mstsc.exe** (*Start >> All Programs >> Accessories >> Communications >> Remote Desktop Connection*).

## re-initialize

Refers to the re-initiation of Encentuate Keys (such as the USB Key) for reuse.

## register

Signing up for an Encentuate account, and registering a second factor (e.g., USB Key, RFID) with IMS Server.

## reset

Refers to resetting the authentication factors for an Encentuate Wallet (offline or online). Offline resets allow a user to reset his wallet while offline.

## revoke

Refers to removing access to an Encentuate Key so it can no longer be used as an authentication factor for a Wallet.

## secret

Information known only to the user.

## secret question

A question where the answer is known only to the user. As part of Encentuate's Knowledge-based authentication, users will be asked a number of secret questions.

## security officer

An officer that defines the identity wallet security policies and other application policies.

## serial number

A unique number embedded in the Encentuate Keys, which is unique to each Key and cannot be changed. For a USB Key, the serial number is printed on the casing of the Key.

## service locator

Refers to the address/path/URL of any logical system that provides back-end shared computing services. AccessStudio uses the service locator to differentiate between different services that a user may be accessing, some of which may use the same client-side application.

### **sign-on automation**

A technology that works with application user interfaces to automate the sign-on process for users. Many ESSO products use this technology to achieve SSO—users log onto the sign-on automation mechanism and the sign-on automation system takes over from there to log the user onto all other applications.

### **signup**

Requesting for an account with the IMS Server. As part of the process, users are issued an Encentuate Wallet. They can subsequently register one or more second factors with the IMS Server.

### **single sign-on**

A capability that allows a user to enter a user ID and password to access multiple applications.

### **SSL**

Secure Sockets Layer

### **strong digital identity**

An online persona that is difficult to impersonate, possibly secured by private keys on a smart card. These identities typically have to be supported by physicalized authentication factors.

### **token**

A small, highly portable hardware device that the owner carries to authorize access to digital systems and/or physical assets.

### **USB Key**

A portable and personalized device for storing user names, passwords, certificates, encryption keys, and other security credentials.

### **user-centric, server managed**

A distributed, agent-based system that provides the user with the convenience of a user-focused agent, and provides the enterprise with consolidated views and controls over the distributed agents. If designed carefully, it can avoid the pitfall of many distributed systems — a single point of failure in the server.

Encentuate IAM has a user-centric, server-managed architecture in which the AccessAgent provides access security functions to the users, and is centrally managed through the IMS Server.

### **user name (user ID)**

A unique identifier that differentiates the user from all other users in the system.

### **User role**

A role that is required to use AccessAgent for sign-on automation. This is one of the three Encentuate Predefined Roles within the Encentuate IAM system.

### **Virtual Challenge Response (VCR)**

A method for authentication using an out-of-band (virtual) challenge, and where the response to the challenge leverages an application's password authentication method (e.g. RADIUS) for authentication. It allows an organization to migrate to certificate-based authentication without changing an application's existing authentication mechanism — minimizing integration requirements.

### **Wallet**

An identity wallet that stores a user's access credentials and related information (including user IDs, passwords, certificates, encryption keys), each acting as the user's personal meta-directory.